RESUMEN DEL PROYECTO:

El presente proyecto fin de carrera tiene como objetivo realizar un estudio del núcleo de red en las de redes de nueva generación (NGN) y de cómo la evolución de las redes actuales hacia estos conceptos producirá un cambio en la forma de pensar y desarrollar las redes de comunicaciones del futuro.

El estudio esta desglosado en tres grandes partes y se inicia con el análisis de la evolución que ha sufrido el núcleo de red en las redes de comunicaciones móviles digitales desde la implantación de las primeras redes digitales hasta la actualidad abarcando tanto la evolución de las redes troncales como de las redes de acceso así como los cambios que han tenido lugar tanto dentro de las propias estructuras de red de los operadores como la forma de interconectarse entre sus redes.

Una segunda parte que constituye el cuerpo teórico del trabajo donde se estudia a nivel funcional y de arquitectura de red el desarrollo de los nuevos modelos de red proporcionados por los organismos de estandarización que dan lugar a la aparición de las redes de nueva generación (NGN) y que constituirán el siguiente paso en la evolución de las redes de comunicaciones hacia una infraestructura de red común para todas las redes de acceso actuales.

Y una tercera parte que tiene como objetivo el estudio del grado de transformación que tienen que sufrir el núcleo de red en actuales redes troncales de comunicaciones móviles y terrestres, así como una valoración del estado actual de dicha integración, de las dificultades que están encontrando fabricantes y proveedores de servicio para la implementación de dichas redes en el contexto tecnológico y económico actual y su respectivo análisis de como afectará este cambio a los modelos de negocio de los proveedores de servicios de telecomunicaciones. Finalmente se estudia como se esta llevando a cabo este proceso por medio de un caso práctico de implantación e interconexión de la solución propuesta por un fabricante de equipamiento basándose en los modelos anteriormente expuestos en una red comercial de un operador en España y todas las implicaciones asociadas a esta caso concreto.

ABSTRACT:

The object of this work is to provide a deep view about the core network inside next generation network (NGN) and how the evolution of the current comunications networks towards the concepts introduced by these new networks brings a change in the way of think and develop communications networks of the future.

This work is composed of three blocks and one real case and it starts with the analysis of the evolution of the core network in digital mobile comunications networks since the beginning of the digital mobile comunications networks deployments until nowadays both in core network side and access network side and how the providers have made changes inside their comunications infrastructure and how they interconnect them with other networks.

A second part which is the central theoretical part of this work where it is studied the next generation network models stablished by telecomunications associations and how they will be the next step in the evolution of comunications networks towards a common network infrastructure for all existing access networks.

A third part where it is studied the level of transformation that core network in mobile and terrestrial comunications networks have to experienced since current situation up to next generation scenarios and what it is the impact of these changes, the issues that are arising for developers, manufactures and service providers in this process, the way that these changes will improve and shift telecomunications business models and how the current economic and technological context is influencing in the whole process.

Finally it is studied a actual case about a proposed solution by a manufacturer that based on the models exposed in second part take place a integration and interconection process in a the comercial network of one telecomunication service providers in Spain. This final part regards to all implications associated with this specific case.

UNIVERSIDAD POLITÉCNICA DE MADRID

Escuela Universitaria de Ingeniería Técnica de Telecomunicación

PROYECTO FIN DE CARRERA

El núcleo de red en redes de nueva generación

Autor: Francisco Javier García Romero

Septiembre 2012

Agradecimientos

A mi familia, por la paciencia y la ayuda que me han dado todos estos años y por su esfuerzo para permitirme estudiar.
A Adriana, por su compresión, su apoyo y su cariño porque sin ella no hubiera encontrado la determinación necesaria para terminar este trabajo.
Y por último a Jose Miguel por su inestimable colaboración y sus aportaciones y su buena disposición durante el desarrollo de todo este trabajo.

Índice de Contenidos

Memoria

Memoria

1. Análisis de la evolución de las redes móviles

1.1. Introducción

Históricamente el despliegue y evolución de las redes de comunicaciones se ha venido desarrollando bajo el paradigma de que cada servicio ofrecido era proporcionado por un red dedicada a dicho servicio, que comprendía un tipo de terminales concretos, que se conectaban a una red de acceso cerrada y perfectamente definida y esta a su vez, se conectaba a una red troncal que interconectaba a los usuarios entre si y proporcionaba dicho servicio. Este paradigma de un servicio por cada infraestructura implicaba una serie de importantes desventajas como unos elevados costes de inversión en el despliegue y el mantenimiento de dichas redes así como una creciente complejidad según aumentaba el número de usuarios, el tamaño de la red y una limitada capacidad para generar nuevos ingresos por parte de los proveedores de red puesto que cada nuevo servicio requiere del uso de nueva infraestructura.

Por lo tanto este desarrollo tradicional de los servicios de comunicaciones en redes diferenciadas llevó al despliegue de redes superpuestas entre sí, es decir, en paralelo a la red de conmutación de circuitos, que soportaba los servicios de voz, se desplegó una red de conmutación de paquetes dedicada a los servicios de datos, donde los servicios seguían estando fuertemente vinculados a la infraestructura de red que los soportaba, dando como resultado el uso de modelos verticales de servicios.

Figura 1. Concepto redes verticales de servicios

1.2. La estructura de las redes móviles digitales terrestres.

El comienzo de las redes móviles digitales terrestres tuvo su origen en el desarrollo del primer estándar de comunicaciones móviles digitales paneuropea denominado GSM primero por el CEPT y posteriormente por el ETSI. Esta norma desarrollada durante los años 80 y principio de los 90 del siglo pasado, dio como resultado el despliegue durante la primera mitad de los años 90 de redes GSM en todo el mundo, redes de segunda generación basadas en dominios de conmutación de circuitos para el soporte de servicios de voz y mensajería corta SMS (en la fase 1, 1991) y capacidades de transmisión de datos a muy bajas velocidades posteriormente (en el año 1994, fase 2) de hasta 14,4 kbit/s [1y 2].

La estructura básica de las redes GSM [3], constaba de tres elementos, una terminal de usuario o estación móvil, un subsistema de acceso radio y una red troncal. El subsistema de acceso radio estaba compuesto por las estaciones base o BTS que controlan una o varias celdas o áreas de cobertura y un conjunto de controladoras de estaciones base, llamados BSC, que gestionan las estaciones base y todas las funciones de subsistema radio.

Por otro lado estaba la red troncal o backbone, basada en un dominio de conmutación de circuitos compuesta por los MSC o centro de conmutación móvil donde se realiza la gestión y el control de las llamadas en la red. Esta entidad encargada del control de una o varias controladoras de estaciones base BSC, era también la encargada de las funciones de enrutamiento de las llamadas y el control de movilidad de los usuarios.

Uno de los elementos centrales de la red es la base de datos que almacena toda la información relevante de un suscriptor, el HLR. Entidad que funciona junto con el VLR, elemento que almacena información dinámica de localización de las estaciones móviles y es consultado por las MSCs asociadas (las VLR normalmente esta integradas junto con las MSCs [4]) para localizar y posicionar un terminal.

El GMSC o pasarela de interconexión con otras redes móviles, o redes fijas como la PSTN o ISDN, es la función encarga de adaptar formatos y protocolos de señalización entre redes que utilizan diferentes tecnologías para su interoperabilidad.

Además de todas estas funciones, la red se completa con otras dos importantes funcionalidades, el AuC y EIR que tenían como función servir de soporte a la autenticación, autorización, privacidad y seguridad del suscriptor y de su estación móvil dentro de la red del operador [3].

La agrupación y extensión de todas estas entidades de la red de acceso y la red troncal en un área geográfica daba lugar a una red mallada donde los elementos se interconectaban entre sí según su nivel jerárquico para extender el área de cobertura de la red móvil como se puede apreciar en la siguiente figura.

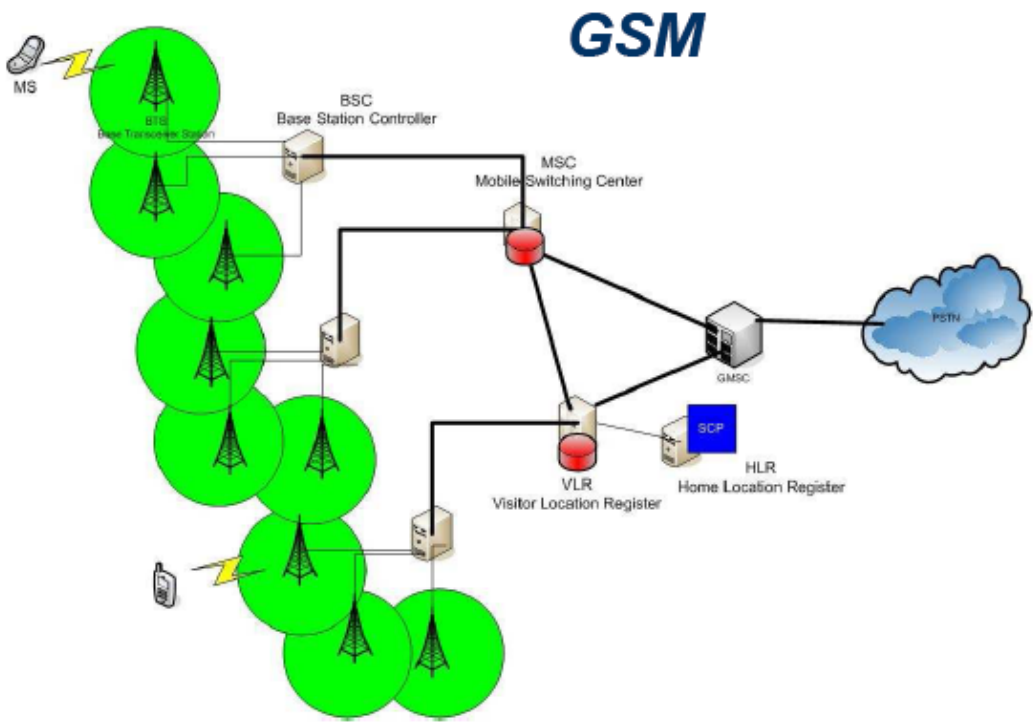

Figura 2. Arquitectura simplificada de la red GSM

1.3. Dominio de datos en las redes móviles digitales

1.3.1. GPRS

La imposibilidad de soportar servicios de datos en la red GSM debido a que sólo soportaba el envío de éstos a unas velocidades de transmisión muy bajas hizo necesario el despliegue de una nueva infraestructura de red que permitiera mayores capacidades de transmisión de datos. Esta nueva infraestructura conocida como GPRS (fase 2+ de GSM 1997-1998 o 2.5G) supuso la integración de una red troncal de conmutación de paquetes superpuesta con el dominio existente de conmutación de circuitos de la red GSM, que proporcionaba acceso a redes basadas en el protocolo IP y por lo tanto acceso a Internet desde los terminales móviles permitiendo aumentar el conjunto de servicios móviles disponibles. La red troncal GPRS incorpora un conjunto de nodos superpuestos pero independientes del dominio de circuitos, compuesto por el SGSN como nodo de establecimiento y control de la conexión lógica entre la red y la estación móvil y el GGSN como nodo encargado de proporcionar conectividad IP al terminal móvil para su interconexión con otras redes de datos. Mientras tanto en el nivel de acceso se realizan actualizaciones de software que permiten la gestión de paquetes en la interfaz aire denominada CCU y un nuevo modulo de gestión de paquetes dentro de la BSC, llamado PDU [5].

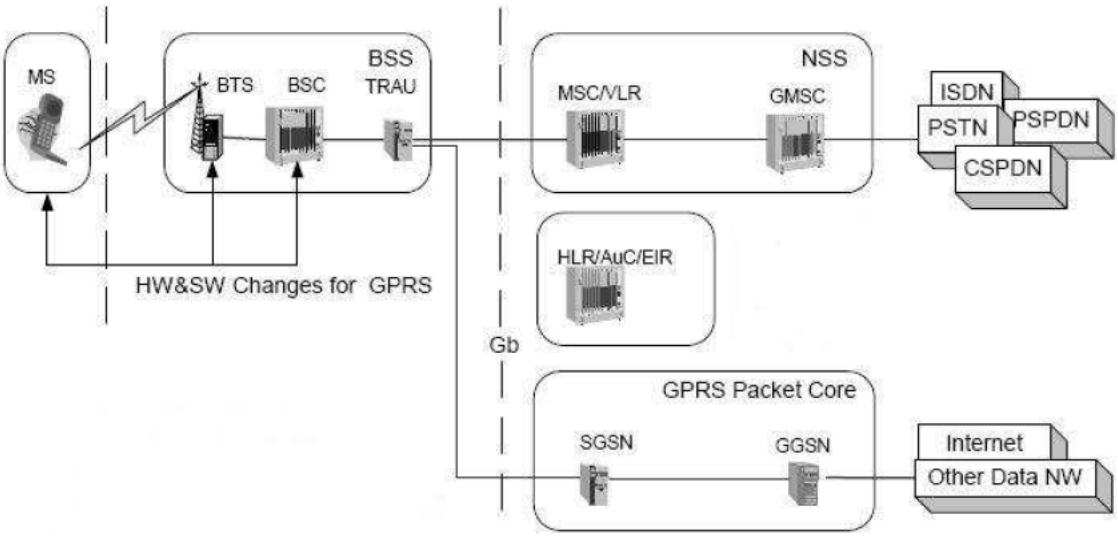

Figura 3. Arquitectura simplificada GSM/GPRS

Esta figura ilustra claramente la diferenciación de infraestructuras que soportan dentro de una misma red cada servicio, donde se impone una organización vertical o semi-vertical de los servicios.

1.3.2. EDGE

Es una importante optimización de GPRS para incrementar las velocidades de transmisión en el interfaz aire y la capacidad de transferencia de datos en la red de acceso, por medio de la incorporación de un transceptor en la estación base y una actualización de software en la red de estaciones base BTS y controladoras de estaciones base BSC. Introducida en la Release 99 de 3GPP da lugar a la evolución de la red de acceso tradicional a la red GERAN donde se puede dar velocidades de transmisión máximas de 470kbps. Fue un paso intermedio para la adaptación de las redes GSM/GPRS en su evolución hacia las redes de tercera generación [3].

1.4. Evolución de los estándares de Redes móviles de 3ª Generación.

Ante las desventajas que presentaba la diferenciación en dominios separados de las redes móviles y las dificultades para proporcionar nuevos y más interesantes servicios de comunicaciones a través de las mismas, a finales del siglo pasado se creo, el grupo de trabajo 3GPP (compuesto por los organismos de estandarización ETSI (European Telecommunications Standard Institute) junto con las organizaciones regionales de estandarización de EEUU (T1) , Japón (TTC y ARIB), Corea del Sur (TTA) y China (CCSA)) para el desarrollo de la siguiente generación de redes móviles (3G). Este grupo asumió el desarrollo de una nueva red que diera respuesta a la necesidades de una red global que facilitara acceso a servicios de voz, datos y multimedia por medio de una conexión de banda ancha de alta velocidad y a través de una

plataforma que resolviera las limitaciones de las redes de móviles de segunda generación GSM/GPRS.

1.4.1. Release 99

La primera especificación de UMTS, o red de tercera generación, fue la Release 99 o Release 3 (R3) de 3GPP, que tenía como principal novedad el desarrollo de una nueva red de acceso de banda ancha, conocida como UTRAN, que permitiera que las tasas de transferencia de datos en la interfaz aire crecieran de manera muy significativa, proporcionando conexiones de datos de alta velocidad a los terminales móviles de hasta 2Mbps [5]. Esto se consiguió a través del uso de nuevas técnicas de espectro ensanchado como WCDMA en la interfaz aire entre el terminal de usuario y la estación base. La nueva red de acceso estaba compuesta de un conjunto de estaciones base que soportaban WCDMA, los Nodos B y un conjunto de controladores de estaciones base llamados RNC.

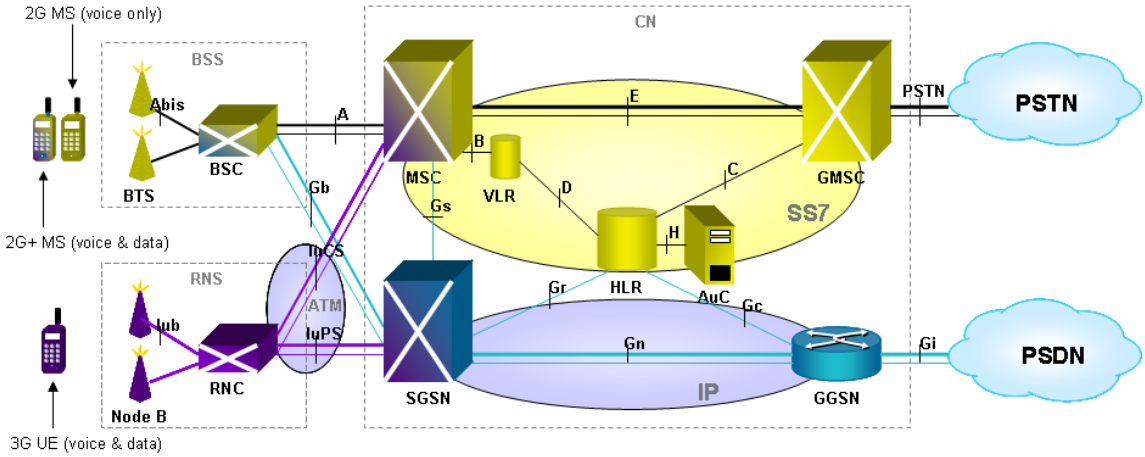

Figura 4. Arquitectura simplificada de una red UMTS. Release-99

Con respecto a la red troncal, la Release 99 no introduce ningún cambio significativo con respecto a las redes de la generación anterior, puesto que se mantiene los dominio de circuitos y de paquetes superpuestos entre sí de las redes GSM/GPRS [3].

Otro aspecto relevante es la introducción de una estructura abierta y flexible de servicios, conocida como OSA que permitía la creación de nuevos servicios multimedia a través de un entorno de gestión común que permitiera el desarrollo de aplicaciones y servicios por proveedores externos de una forma segura, rápida y estandarizada.

1.4.2. Release 4

Con la siguiente especificación llegan los principales cambios sobre el dominio de conmutación de circuitos de la red troncal constituyendo el primer paso en la evolución de la red hacia el concepto de red de nueva generación, estableciendo el uso

de una red de transporte IP o ATM de conmutación de paquetes como red de transporte común, para todos los servicios de la red, incluido los servicios de voz que hasta este momento eran transportados entre las estructura monolíticas de conmutación del dominio de circuitos. Para implementar este cambio se rompe el concepto de dominio de conmutación de circuitos monolítico, separando el plano de señalización del plano de transporte para permitir que los elementos del nivel de transporte se interconecten en una red de conmutación de paquetes IP.

Esto se traduce en la ruptura de las MSC monolíticas, en un nivel de control de llamada o señalización compuesto por las MSC-Server y los GMSC-Server y un nivel de transporte formado por las pasarelas de medios que se integran e interconectan en el nivel de transporte IP, llamados CS-MGW que controlan el tráfico de usuario y realizan la adaptación de las portadoras de medios para su transporte sobre IP o ATM.

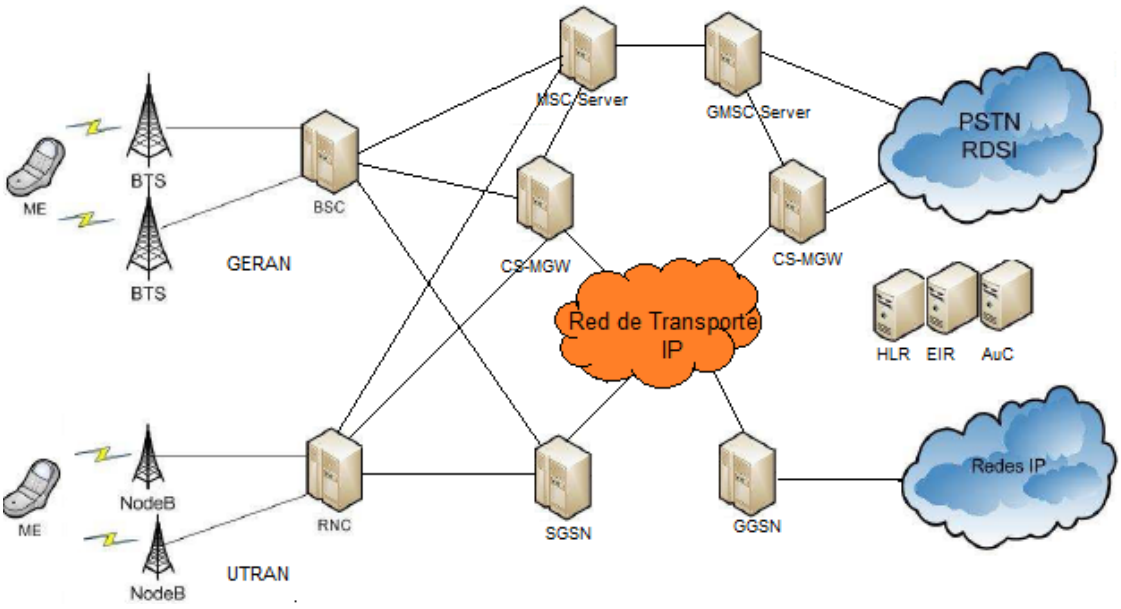

Figura 5. Arquitectura simplificada con red de transporte común Release 4

Las MSC Server serán las entidades encargadas del control de la llamada y del control de la movilidad por medio del intercambio de mensajes de señalización con los elementos de la red de acceso (RNC y BSC) y con otras MSC Server o GMSC Server para la transmisión de señalización a través de la red troncal sobre protocolos BICC o ISUP, de SS7. El MSC Server tiene también como función controlar las pasarelas de medios, CS-MGW a través del protocolo de control de pasarela de medios MEGACO o H.248

El GMSC Server no es más que otra MSC Server que se encarga de la intercambio de mensajes de señalización SS7 (ISUP, TUP u otros) de llamadas con otros dominios de conmutación de circuitos como PSTN o ISDN.

La pasarela de medios CS-MGW es la entidad encargada de las funciones de transmisión del tráfico de voz de la llamada. Por un lado se interconecta con los elementos de la red de acceso RNC/BSC de lo que recibe los canales de portadoras de voz y convierte y adapta a flujos de medios para ser retransmitidos sobre la red de transporte de conmutación de paquetes RTP/UDP/IP o AAL2/ATM. Los flujos se transmiten por esta red de transporte y llegan a otra pasarela de medios que bien

conectará con la red de acceso radio, haciendo el proceso inverso al anterior o con una pasarela de medios CS-MGW que se interconecta con las redes fijas tradicionales (PSTN o RDSI). Por lo tanto esta entidad realiza de la adaptación de los protocolo de medios (de RTP a TDM o AAL2 o viceversa) y de las características propias de cada medio como la codificación, (adaptación de codificación GSM o AMR a PCM u otros), cancelación de ecos, etc.

1.4.3. Release 5

La siguiente especificación de 3GPP introdujo por primera vez el concepto de subsistema multimedia IP o IMS en sus siglas en inglés, como la evolución de las redes troncales hacia una plataforma de control común para la entrega de servicios multimedia sobre el dominio de conmutación de paquetes de transporte desplegado en las redes móviles 2.5G y 3G con un cierto nivel de calidad de servicio garantizado. Se trata por tanto, de una plataforma que incorpora las funciones de señalización y control, para la conexión, modificación y finalización de sesiones multimedia entre usuarios y servicios, basada en las tecnologías y protocolos utilizados en las redes de datos y que utiliza como red de transporte para los datos de usuario, la red de conmutación de paquetes IP de la red UMTS, para el transporte y distribución de los servicios actuales y de nuevo desarrollo.

La evolución hacia una única red de transporte IP, lleva hasta la red de acceso UTRAN, el transporte sobre conmutación de paquetes, sustituyendo los enlaces punto a punto TDM actuales entre los nodos, por conectividad IP entre ellos, extendiendo el concepto de redes de datos a toda la arquitectura de la red.

Finalmente se introduce una mejora en la interfaz entre la red de acceso y terminal de usuario que mejora la capacidad de transferencia en la interfaz aire, a través de HSDPA, que es una mejora de la técnica de espectro ensanchado de UMTS, WCDMA, que básicamente incorpora un nuevo canal de transporte en el enlace descendente en conjunción con nuevas técnicas de modulación, codificación y retransmisión, sobre los nodos de la red de acceso (RNC/NodoB) para permitir velocidades de transmisión de hasta 14 Mbps teóricos en el enlace descendente (unos 3/4 Mbps reales).

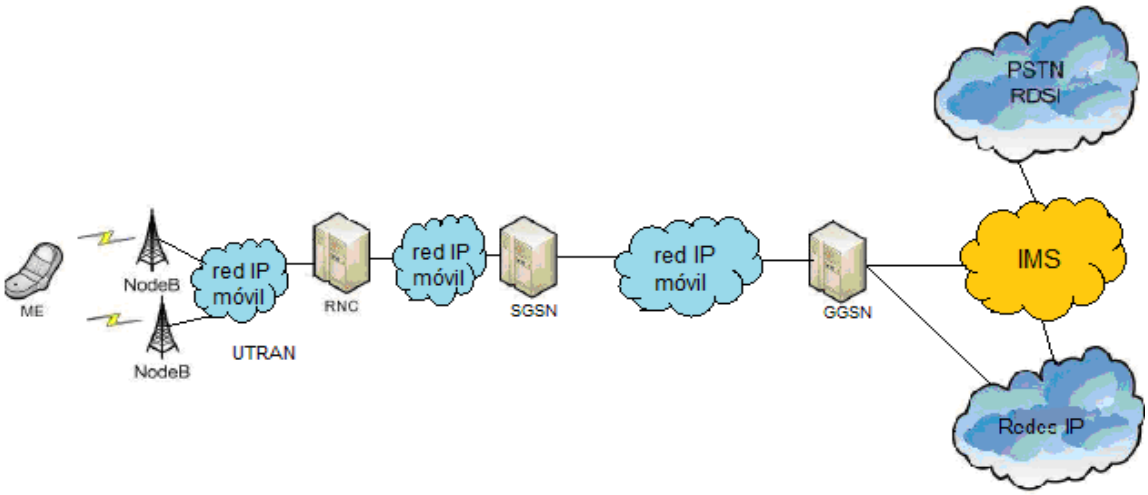

Figura 6. Arquitectura simplificada de red móvil en Release 5

1.4.4. Release 6

En la siguiente especificación se produce una profundización en el desarrollo y las funcionalidades del nivel de control incorporado en la Release 5, IMS, profundizando en algunos conceptos ya introducidos como la separación cada vez mayor entre los planos de transporte y control y la introducción de un nueva característica principal en las redes de nueva generación, la independencia del tipo de red de acceso por el cual se accede a la red multimedia, introduciendo la interconexión con terminales de usuario a través de redes inalámbricas WLAN por medio de una pasarela de datos que se comunica con los niveles de transporte y control como se muestra en la figura 7.

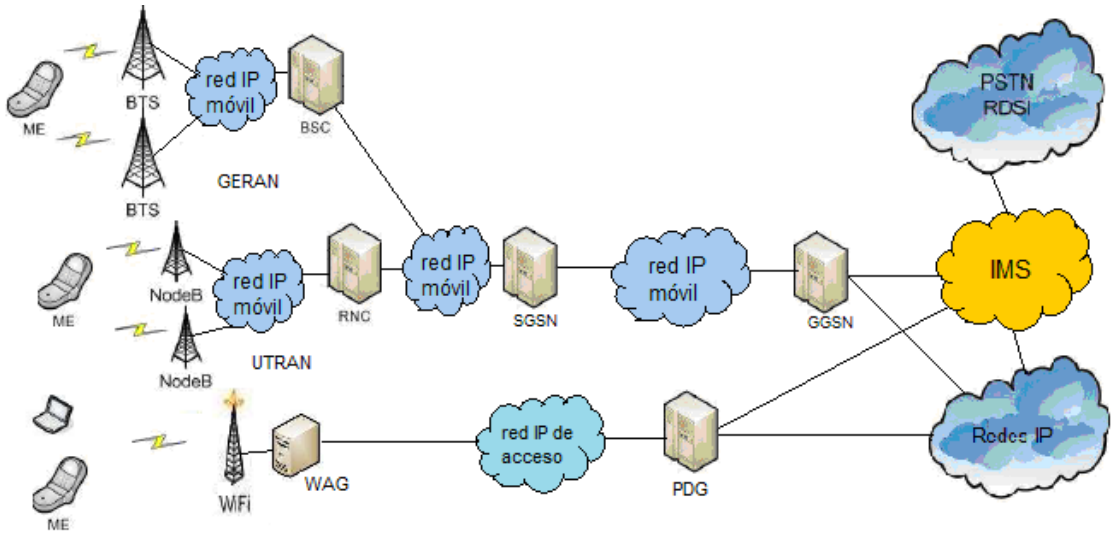

Figura 7. Arquitectura simplificada con redes de transporte IP e introducción de acceso inalámbrico. Release 6

Una de las características más importante es la incorporación de nuevas redes de acceso que permitirán el acceso a los servicios proporcionados por la red multimedia a través de los dominios de conmutación de paquetes anteriormente descritos, lo que se traduce en el primer intento de convergencia del estándar de 3GPP con otras redes de comunicaciones existentes. En este sentido se produce el primer acercamiento para la armonización de los diferentes estándares que estaban desarrollando los diferentes grupos de estandarización en redes móviles, en este caso con la organización 3GPP2 (grupo de trabajo promovido por las agencias norteamericanas TIA y ANSI encargado de la evolución de las redes móviles basada en el estándar CDMA2000 [7]) y las primeras especificaciones de este grupo, 3GPP2 MMD-0 y MMD-A hacia arquitectura de redes multimedia de nueva generación muy similar al que desarrolla el 3GPP.

También introduce una actualización en la transmisión en la interfaz aire con la técnica HSUPA que incorpora un nuevo canal de transporte de datos en el enlace ascendente que amplía la capacidad de transmisión hasta los 5,74Mbps teóricos (1.5-2 Mbps reales), mejorando el uso de los recursos radio y disminuyendo el retraso en la transmisión.

1.4.5. Release 7

La Release 7 del 3GPP introduce mejoras fundamentalmente en la interfaz radio de la red de acceso, optimizando el rendimiento y la capacidad de la transmisión radio de hasta 28Mbps/11Mbps en cada enlace con la técnica HSPA+, la cual es una combinación optimizada de las técnicas de transmisión de las especificaciones anteriores en los enlaces ascendentes y descendentes, HSDPA y HSUPA, reduciendo los valores de retardo y distorsión en la comunicación que aumentan la calidad de servicio con el objetivo de introducir nuevas aplicaciones en tiempo real.

Estas características se consiguen a través del empleo de múltiples antenas (MIMO) tanto en el receptor como en el transmisor aprovechando la propagación multitrayecto en la interfaz radio y el uso de modulación de alta eficiencia espectral (64QAM).

En esta versión también se produce la primera especificación de conectividad con redes de acceso fijas o cableadas abriendo la puerta al concepto de convergencia entre redes fijas y redes móviles. Esta adaptación comienza con los trabajos del grupo creado por ETSI para las normativas de redes de comunicaciones cableadas, TISPAN y que tiene como objetivo la adopción de un modelo de red de nueva generación donde los niveles de trasporte, control y servicios son independientes entre sí y donde el transporte se realiza sobre redes IP que faciliten el desarrollo de nuevos servicios y la adaptación de los ya existentes como subsistemas del nivel de servicio (ETSI TISPAN Release 1).

Estos trabajos de armonización con los grupos de trabajo de 3GPP2 y TISPAN permiten que se inicie una compatibilidad en las comunicaciones entre redes y sistemas anteriormente incompatibles (redes móviles, inalámbricas y fijas) y que avancen hacia un modelo común de red troncal compartida e independiente del nivel de servicios y de las tecnologías de acceso utilizadas.

1.4.6. Release 8

Hasta ese momento, diferentes organismos de estandarización (ETSI TISPAN, 3GPP2, WiMax Forum, Cable Labs, el propio 3GPP etc.) habían llevado a cabo sus propios trabajos para la interconexión/evolución de las diferentes redes de comunicaciones existentes (redes móviles de 3ª generación, rede fijas de banda ancha xDSL, redes inalámbricas Wi-Fi, redes inalámbricas basadas en enlaces de microondas (WiMAX), redes de fibra óptica) con modelos de redes multimedia de nueva generación. Desde este momento los grupos de trabajo de 3GPP asumen el desarrollo de las interconexiones con otras redes de acceso diferentes a GSM/GPRS/UMTS, en un esfuerzo de la industria por aunar todos los trabajos de estandarización existentes de los organismos mencionados en un modelo común de red multimedia de nueva generación, con el fin de simplificar las estandarizaciones existentes y hacerlas compatibles entre sí, ampliando el concepto de independencia entre las tecnologías de acceso a la red y los servicios proporcionados por la red troncal, introducido en la Release 6 unos años antes.

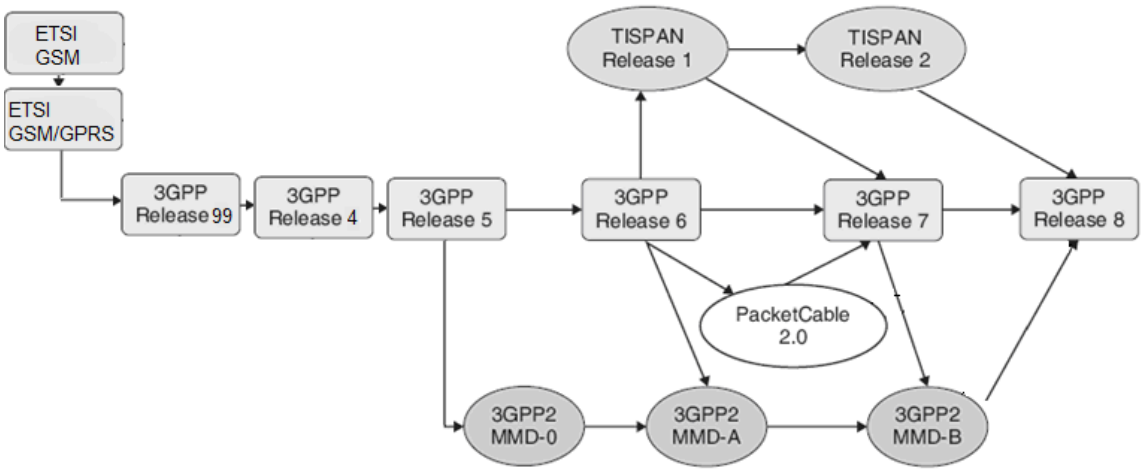

Figura 8. Proceso de evolución y unificación llevado a cabo por los diferentes grupos de trabajo.

Teniendo en cuenta lo anterior y desde el punto de vista de la evolución de la red 3G, en esta especificación tienen lugar importantes cambios en la arquitectura de toda la red móvil, tanto en la red de acceso como en la red troncal.

En la red de acceso, hasta este momento la principal novedad había sido la introducción de nuevas y mejores técnicas de espectro ensanchado (WCDMA, HSDPA, HSUPA, HSPA+) con la llegada de las redes móviles de tercera generación, que permitían el aumento de las capacidades de transmisión y la reducción de retardos y errores en la transmisión sobre la interfaz radio con el objetivo de proporcionar a los usuarios conectividad de banda ancha en sus terminales móviles. Este objetivo, sólo cumplido parcialmente, se intenta impulsar definitivamente con la definición de una nueva y potente interfaz radio en la red de acceso, conocida como LTE, que emplea nuevas técnicas de acceso al medio de espectro ensanchado como OFDMA, que utiliza portadoras ortogonales en frecuencia con una elevada protección contra interferencia multitrayecto, el uso de múltiples antenas con técnicas MIMO en los transceptores de las estaciones base y de las estaciones móviles y una arquitectura de red simplificada, que explicaremos a continuación, que permite un incremento importante de las velocidades de transmisión de hasta 100 Mbps/50Mbps [8] en los enlaces descendente/ascendente , una disminución de los retrasos de establecimiento y transmisión en los canales de señalización (<100 ms. [8 y 9]) y datos (~10 ms. [8 y 9]) y una mejora de la eficiencia espectral de hasta 3 veces más que con HSPA [8], operando en las mismas bandas de frecuencias asignadas para UMTS y con portadoras de ancho de banda variable y adaptativo de entre 1,4 MHz y 20 MHz [3].

La introducción de una nueva arquitectura en la red de acceso, llamada E-UTRAN, más simplificada donde desaparecen el controlador de estaciones base, RNC de UMTS y se introducen un nuevo tipo de estaciones base denominadas E-NodeB, mucho más sofisticadas y que asumen parcialmente las funciones de las antiguas RNCs como el control de los recursos radio, la gestión de funciones de enrutamiento hacia la red troncal etc. Estos nuevos nodos se conectan entre sí y con la red troncal sobre conexiones IP para el transporte de la señalización y los datos de usuario.

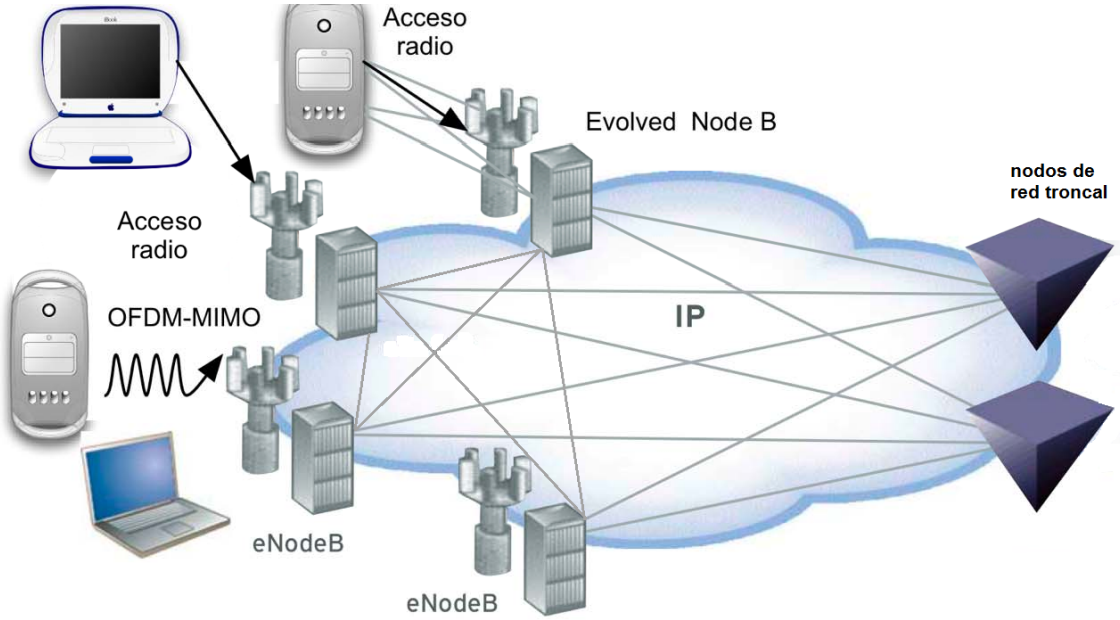

Figura 9. Arquitectura simplificada de la red de acceso en LTE

En la red troncal también se produce una evolución de la arquitectura de la red con la introducción de un núcleo de red, basado en la evolución de la arquitectura de la red GPRS hacia una única red con conectividad IP extremo a extremo con un nivel de control claramente diferenciado del nivel de transporte y que permita el acceso por medio de diferentes tecnologías inalámbricas, donde todos los servicios son proporcionados por el operador, incluidos los de voz, a través de la red troncal IP, eliminando definitivamente el dominio de conmutación de circuitos que existía en las redes 2G y 3G.

La red troncal será responsable del control y la gestión de la conexión y de la movilidad de los usuarios, así como de todas las funciones propias del nivel de control de la red [10]. El núcleo de red IP, conocido como EPC, incluye 3 nuevos entidades lógicas, el MME o punto de comunicación con la red de acceso E-UTRAN para el plan de señalización que se encarga de las funciones de control de la conexión, de la gestión de la movilidad entre accesos 3GPP y la seguridad entre otras. Este nodo se puede considerar como una versión mejorada y optimizada de los nodos SGSN de las redes GPRS [3,8 y 10]. Y una pasarela EPC-GW compuesta por el SGW que es el punto de interconexión con la red de acceso para el plano de datos de usuario y el PDN-GW o PGW que es el elemento encargado de establecer conexiones externas con otras redes de datos para el acceso a servicios multimedia y proporciona funciones de movilidad entre redes de acceso móviles (GERAN, UTRAN, E-UTRAN) y accesos inalámbricos (WiMax, WLAN) [3,10]. Este nodo se puede considerar como una versión mejorada de los nodos GGSN de las redes GPRS. La arquitectura se completa con los servidores de información de suscripción de los usuarios, HSS, que contiene la información relativa a los perfiles de suscripción de los usuarios y de los servicios autorizados en cada uno de ellos. También se incluyen los elementos encargados del control y aplicación de las políticas de red del operador y de tarificación o PCRF.

En la red troncal EPC se integran diferentes redes de acceso que utilizan diferentes tecnologías que satisfacen el concepto de independencia entre las tecnologías de acceso y el nivel de servicio y el transporte sobre un dominio de conmutación IP común a todas ellas [11].

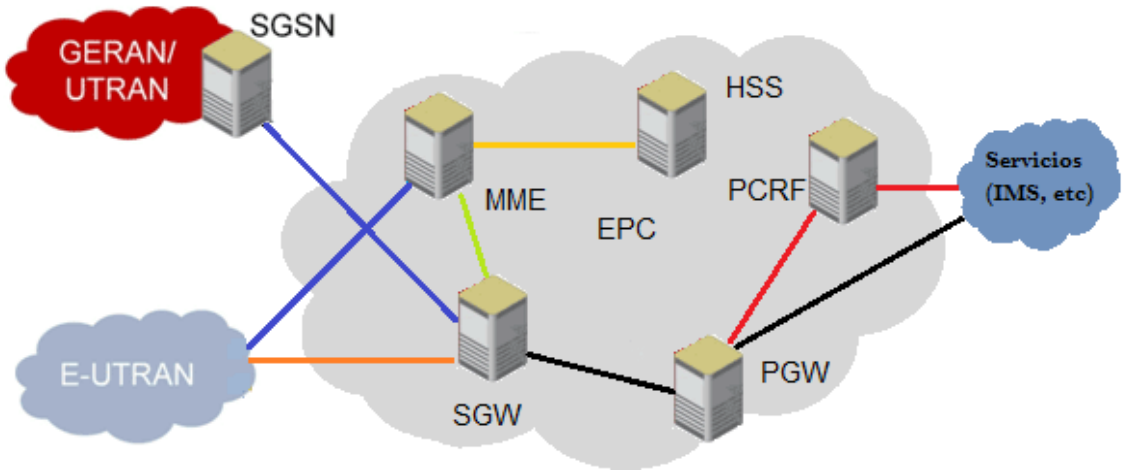

Figura 10. Arquitectura simplificada EPC

El despliegue de la red troncal simplificada de nueva generación EPC y la red de acceso E-UTRAN en combinación con las nuevas técnicas de transmisión empleadas en la interfaz aire conforman el nueva arquitectura de redes móviles denominada EPS.

La Release 8 también incluye una mejora de la interfaz radio para UMTS con la introducción del concepto portadora doble en HSDPA, una actualización en las estaciones base de la red de acceso que permite la transmisión con HSDPA en dos portadoras adyacentes de 5Mhz de ancho de banda en el misma banda de frecuencias en el enlace descendente que incrementan las velocidades de transmisión hasta los 42 Mbps en dicho enlace en combinación con modulaciones de alta eficiencia (64QAM) y sin necesidad de utilizar antenas múltiples [12].

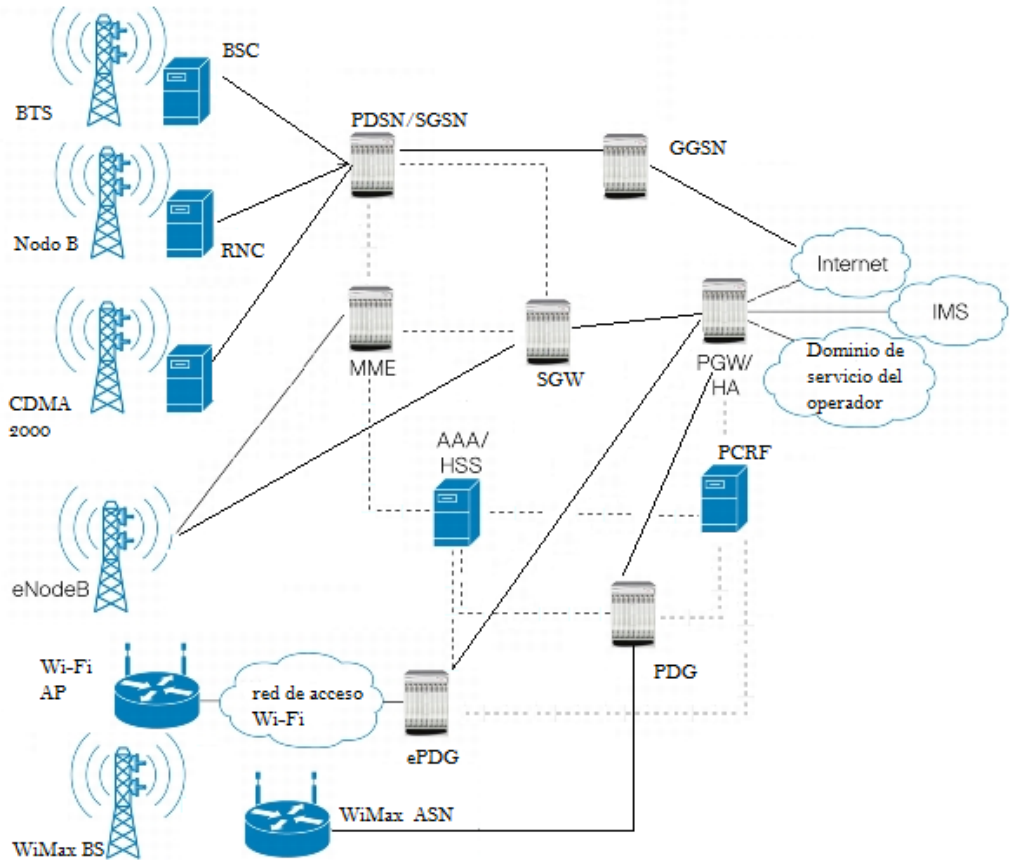

Figura 11. Arquitectura completa EPC/GPRS y su interconexión con otras redes de acceso.

1.4.7. Release 9

Después de la introducción de LTE en la Release 8, los siguientes trabajos en la Release 9 se centran fundamentalmente en la evolución de la técnica HSDPA de portadora doble hacia una técnica de banda doble, donde cada una de las portadoras se encuentran en bandas de frecuencias separadas y destinada a aquellos operadores que por no disponer de bandas de espectro adyacentes no pudieron desarrollar la transmisión en el enlace descendente sobre portadora doble. También introduce la combinación de la técnica de portadora doble HSDPA con más de una antena (MIMO) para aumentar las velocidades de transmisión hasta los 84 Mbps e incrementar la eficiencia espectral significativamente [12]. Para terminar incorpora las mejoras implementadas para el enlace descendente al enlace ascendente con la técnica de portadora doble en HSUPA para doblar las velocidades de transmisión hasta los 23 Mbps [12].

Con respecto a EPS se producen pequeñas mejoras con respecto a lo definido en la especificación anterior, en la interfaz radio LTE se optimizan los canales de transporte, interfaces y otros y se incorpora una solución de mejora de cobertura LTE en entornos cerrados (edificios) con el Home E-NodeB [13]. En la red troncal se añaden características adicionales en IMS como servicios de emergencia, servicios de localización, servicios de voz sobre paquetes que provocan una evolución en la arquitectura IMS (incorporación de nodos de control específicos de sesiones de emergencia etc.) [12 y 13].

1.4.8. Release 10

Durante el transcurso de la creación de la especificación 9 de 3GPP, la Unión Internacional de Telecomunicaciones, ITU en sus siglas en inglés, establece la definición de redes móviles e inalámbricas de 4ª Generación, a través del grupo de radiocomunicación IUT-R, estableciendo el conjunto de características que deberán cumplir las diferentes tecnologías que vayan surgiendo para convertirse en la nueva generación de redes inalámbricas de comunicación 4G conocido también como IMT-Advanced.

Esta definición se basa en algunos conceptos básicos ya incorporados en anteriores especificaciones de redes de nueva generación como redes troncales y de interconexión de conmutación IP con velocidades de transmisión de hasta 1Gbps en condiciones semiestacionarias y hasta 100 Mbps en condiciones de movilidad a alta velocidad, con anchos de banda escalables de hasta 40 MHz [14 y 15], elevados valores de eficiencia espectral de pico de 6 a 15 bps/Hz [13] para la optimización de los recursos de red y la posibilidad de soportar más conexiones y usuarios por cada celda de cobertura para la transmisión de servicios móviles multimedia de muy alta calidad como servicios de difusión IPTV o HDTV.

La Release 10 surge como la respuesta de 3GPP para adaptar el estándar de radio LTE definido en las Release 8 y 9, hacia un estándar que cumpla con los requisitos requeridos por ITU-R para ser considerado como el estándar de nueva generación que permita velocidades de transmisión de hasta 1Gbps en la interfaz radio en el enlace descendente, en anchos de banda adaptativos y escalables de 20 MHz a 100 MHz a través del uso de múltiples portadoras en LTE, en analogía a lo realizado sobre HSPA+ anteriormente, en combinación con el uso de múltiples antenas (MIMO) y el uso de técnicas de disminución de interferencia entre celdas de cobertura y técnicas de recepción y transmisión desde y hacia múltiples celdas que proporcionan eficiencias espectrales de pico de 15-30 bps/Hz [13]. El nuevo estándar conocido como LTE–Advanced deberá establecer compatibilidad hacia las especificaciones anteriores permitiendo una migración suave y flexible desde los sistemas con las primeras especificaciones de LTE hacia sistema avanzados y permitir una sencilla y fácil interoperabilidad y movilidad con otras redes de acceso inalámbricas como WLAN o WiMax.

1.4.9. Release 11

La Release 11 de 3GPP, actualmente abierta y en progreso y prevista para finales de 2012 tiene como objetivos seguir con el desarrollo de LTE-Advanced y la integración con servicios IP avanzados a través de las interconexiones entre operadores y proveedores.

2. Redes de nueva generación (NGN)

2.1. Introducción

Debido al desarrollo y madurez de las tecnologías de la información y de comunicación que se ha alcanzado desde mediados de la década de los 90 hasta hoy en día y muy especialmente al desarrollo masivo e imparable de Internet y de todas las tecnologías asociadas con ésta, ha sido posible la extensión de conceptos hasta hace no mucho nunca vistos por los usuarios de las redes de comunicaciones donde la conectividad global, la flexibilidad de acceso, libertad de elección de servicios y la variedad de los mismos elevan casi hasta el infinito las posibilidades que ofrecen las redes de comunicaciones del futuro. Es en este momento cuando los agentes involucrados empiezan a entender las oportunidades que pueden aparecen con la creación de redes de comunicaciones que proporcionen acceso a un número cada vez mayor de usuarios que acceden a todas las posibilidades que ofrece el mundo de Internet con la calidad de servicio, la fiabilidad y disponibilidad de las redes de comunicaciones tradicionales habilitando el desarrollo de nuevos y avanzados servicios de comunicaciones para los usuarios y nuevos modelos de negocio para los operadores y proveedores de telecomunicaciones e Internet. Todo esto muy relacionado a un conjunto de factores importantes como la necesidad de reducir costes en los servicios tradicionales, la necesidad de ampliar el rango de servicios ofrecidos para incrementar los ingresos, la búsqueda de simplificación y unificación de operación y mantenimiento de los servicios y las redes actuales o la búsqueda de la mejora de la eficiencia de las inversiones realizadas, con el fin de aumentar la competividad por parte de los operadores y aumentar su cuota de mercado en un entorno de fuerte competencia, ha llevado al desarrollo de un nuevo paradigma de red de comunicación que aúna lo mejor de la madura, fiable y cualitativa industria de las telecomunicaciones con las posibilidades y el crecimiento de Internet.

2.2. Definición

Podemos definir el concepto de red de nueva generación muy simplificadamente como una red de banda ancha de conmutación, con unas funcionalidades de transporte y control común, que permite el desarrollo de servicios de forma estandarizada e independiente con respecto a la arquitectura de la red y que integra e interconecta múltiples redes de comunicaciones de acceso a través de las cuales proporciona un amplio espectro de servicios de telecomunicaciones. Por lo tanto podemos decir que se trata de un modelo de red común de banda ancha multiservicio, multiacceso, con calidad de servicio, segura, flexible y fácilmente escalable.

2.3. Características fundamentales

2.3.1. Red troncal de conmutación de paquetes

La red troncal común se desarrolla sobre el concepto de una red de conmutación de paquetes sobre el protocolo de Internet desarrollado por el grupo IETF que permiten

la convergencia con el mundo de Internet a través del tan extendido protocolo IP, puesto que este tipo de redes proporcionan una mayor eficiencia del uso de los recursos de la red, un mayor velocidad de conmutación, y una comunicación más fiable al poder establecerse caminos alternativos, creando una infraestructura que responda a los criterios, fiabilidad, capacidad, disponibilidad, flexibilidad y escalabilidad.

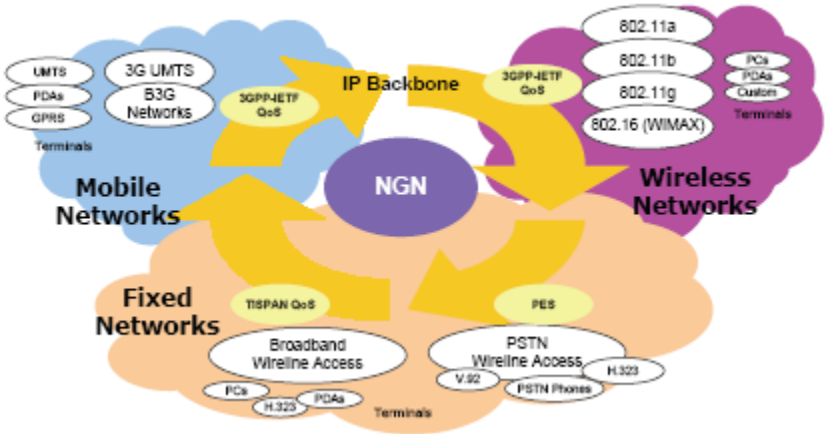

Figura 12. Modelo de NGN basado en una red de conmutación IP común a múltiples accesos.

2.3.2. Arquitectura y estratificación

La arquitectura de red troncal se basa en la organización de la red en una arquitectura horizontal, donde la red está diseñada en diferentes niveles horizontales lo más independientes entre sí posible para que las funciones de los niveles superiores no dependan de los niveles inferiores, facilitando la escalabilidad de los diferentes niveles.

Podemos estratificar las redes en varios niveles diferenciados:

- Un primer nivel de acceso y transporte, que consta de dos subniveles, el primero que comprende las diferentes redes de acceso empleadas para acceder a la red troncal, donde cada red de acceso utiliza su propia tecnología y sus propias reglas de comunicación entre el terminal del usuario y los elementos de la red de acceso y un subnivel de transporte común a todos los usuarios (IP en este caso) y que interconecta las redes de acceso con las funciones principales del nivel de control y proporciona la comunicación entre usuarios y el acceso a los servicios.
- Un segundo nivel de control, que consta de todas las funciones principales de la red, como establecimiento, control y finalización de sesiones, control de servicios y usuarios, facturación, seguridad, interconexión con otras redes, calidad de servicio, aplicación de políticas de red etc.
- Y finalmente un nivel de servicio donde se desarrollan y alojan los servicios ofrecidos por el operador o por proveedores externos y que son completamente independientes de las funciones de acceso y transporte. Pudiendo evolucionar de una forma independiente y que tiene una forma estandarizada de comunicarse con los niveles inferiores.

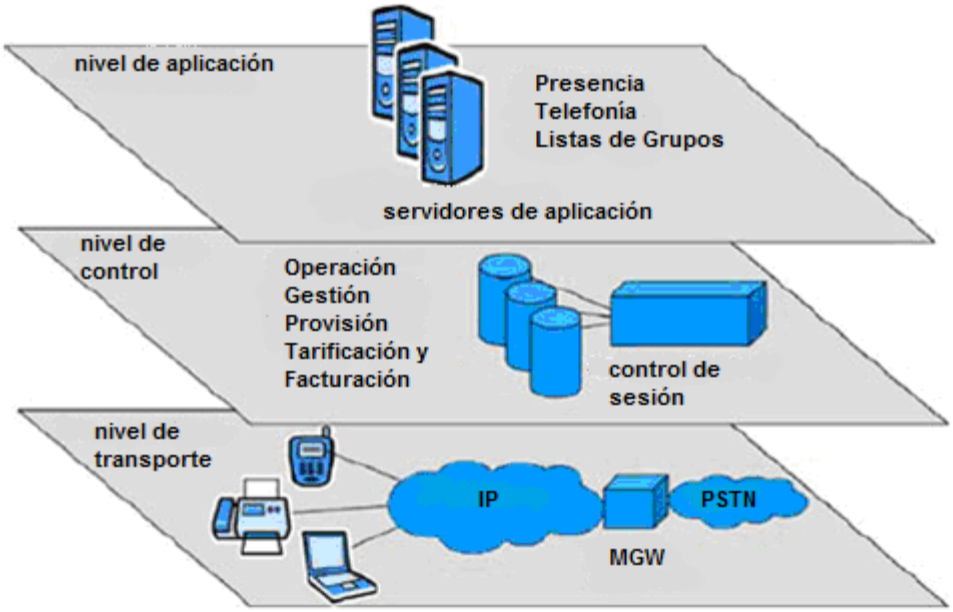

Figura 13. Modelo de red de nueva generación en capas simplificadas

2.3.3. Independencia de servicios

El desarrollo de un nivel de aplicación o servicio, un nivel de control y un nivel de transporte y acceso independientes entre sí permite desligar las aplicaciones y los servicios desplegados, del tipo de red de acceso y del dispositivo o terminal utilizado para acceder al mismo, permitiendo a los desarrolladores centrarse en las cuestiones propias del servicio olvidándose de las consideraciones relativas al tipo de acceso al servicio. Esta simplificación en el desarrollo y en la integración de servicios potenciará la aparición de nuevas y mejoradas funcionalidades con los claros objetivos de aumentar el valor añadido a la red y reducir los tiempos de despliegue de los mismos.

2.3.4. Independencia de red de acceso

Uno de los objetivos de la estratificación de la red en niveles horizontales es conseguir que la red troncal de transporte permita la interconexión y la interoperabilidad entre múltiples redes de acceso de diversas tecnologías, donde la única condición será que todas ellas proporcionen conectividad IP a los terminales de usuarios, tanto con redes de conexión cableada (xDSLs, redes de fibra, redes corporativas) como con las redes móviles existentes (dominios de datos de PLMNs, como GPRS, HSDPA, HSPA+,LTE etc.) como con redes inalámbricas (WLAN, WIMAX, terminales por satélite etc.)

Esta arquitectura multiacceso estandarizada permitirá el establecimiento de sesiones multiservicio con un determinado nivel de calidad de servicio entre usuarios sin importar el tipo de dispositivo y la red de acceso utilizada para conectarse a la red.

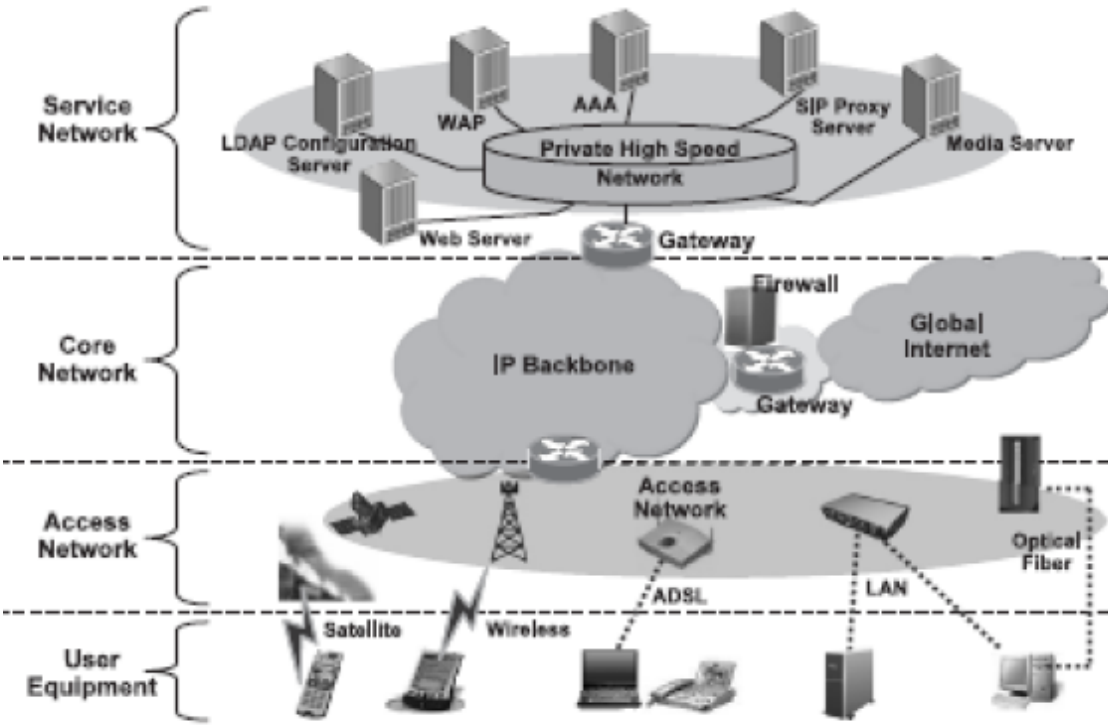

Figura 14. Interconexión con múltiples accesos independientes del nivel de servicio.

2.3.5. QoS

En la red de nueva generación el desarrollo e integración de servicios, sobretodo alguno muy dependiente de los parámetros de calidad, tienen que realizarse en las mismas condiciones de servicio que en las redes de comunicaciones tradicionales donde los estándares de calidad son muy elevados y conforman una pieza fundamental en la experiencia de usuario en la red. La resolución práctica de esta cuestión dependerá de cada implementación concreta y de la solución adoptada por cada operador pero desde luego pasa por ser un criterio clave de diseño de la infraestructura y donde al menos se considerará siempre:

- El tratamiento jerarquizado del tráfico, integrando funciones de clasificación de flujos de datos en distintas clases de tráfico y la asignación de prioridades.
- Se incluirán funciones de monitorización y control del tráfico en la interfaz de cliente y en los diferentes niveles de la red.

2.3.6. Interconexión con redes existentes

Otro requisito fundamental de las redes de nueva generación es que tienen que interconectarse y comunicarse tanto con las redes de comunicación basadas en conmutación de circuitos existentes (red telefónica básica (PSTN), redes móviles terrestres (PLMNs)) como con redes de datos (Internet, GPRS, Redes corporativas, WAN, LAN, etc.) para permitir comunicarse con usuarios de estas redes y ampliar el alcance al mayor número posible de usuarios.

2.3.7. Identificación y seguridad

Otra de las características claves de las redes de nueva generación es la aplicación de los métodos de seguridad más robustos y fiables disponibles en el mundo de Internet y en las comunicaciones móviles etc. Estos métodos serán de aplicación tanto en el nivel de acceso, de transporte, de aplicación como de usuario proporcionando comunicaciones seguras, integras, encriptadas y confidenciales entre usuarios y entre los subniveles de la red.

2.3.8. Beneficios económicos para los operadores

Los beneficios económicos son notables al desarrollar una red que permite dar múltiples servicios a través de una arquitectura única y estandarizada. Los costes de inversión y mantenimiento se reducen al existir una única red de transporte y de control que da servicio a todas las redes de acceso lo que se traduce en una reducción y concentración de las inversiones, aumentando la rentabilidad de éstas puesto que en una red de transporte y control basada en IP, las inversiones realizadas son más eficientes (entre un 15% y un 40 %) [16 y 17] que en las soluciones basadas en conmutación de circuitos.

Por otro lado permite el desarrollo de nuevos servicios que supondrán tanto un menor gasto de integración, debido a que siempre se realizara de una manera estandarizada y simplificada, como un aumento de los ingresos y las posibilidades de negocio puesto que facilitará el desarrollo de nuevos servicios que crearan nuevos usos los cuales aportarán un mayor valor añadido y por tanto una mayor aprovechamiento de la infraestructura.

2.4. Conclusión

El desarrollo de esta red de nueva generación permitirá dejar atrás el hasta ahora dominante concepto de redes verticales donde existía una red por cada servicio, pasando a un nuevo paradigma donde una única red troncal común interconectada a través de los potentes y estandarizados protocolos de red de Internet permita ofrecer todo un conjunto creciente de servicios a diferentes usuarios sin importar el dispositivo y la red de acceso utilizados con un cierto nivel de calidad de servicio, lo que permite aunar lo mejor del mundo de las telecomunicaciones (redes extremadamente fiables y estables y con un elevado nivel de servicio) con lo mejor del explosivo y creciente mundo de Internet creando una herramienta potente y muy interesante desde el punto de vista del usuario, de los operadores de red y de los proveedores de servicio.

3. IMS

3.1. Introducción

La principal implementación técnica que se ha llevado a cabo de una red de nueva generación es IMS (IP Multimedia Subsystem) usando el paradigma de arquitectura horizontal y el modelo de comunicación cliente/servidor tan extendido en el mundo de Internet, que establece las entidades funcionales básicas necesarias de las red troncal y los procedimientos de comunicación necesarios para el despliegue de una red de comunicación que permita el establecimiento de sesiones multimedia y multiservicio entre usuarios y que cumpla con todas las características mencionadas en el capítulo 2.

La solución completa consta de unos terminales con capacidad para establecer conexiones IP con la red, una red de conectividad IP que hace las funciones de transporte y conexión tanto de tráfico de señalización como tráfico de usuario, y finalmente un conjunto de funcionalidades que se encargan del control de la sesión, del usuario y del servicio. El último nivel se encargaría de facilitar un conjunto de servicios de todo tipo proporcionados por el propio operador o por un tercero.

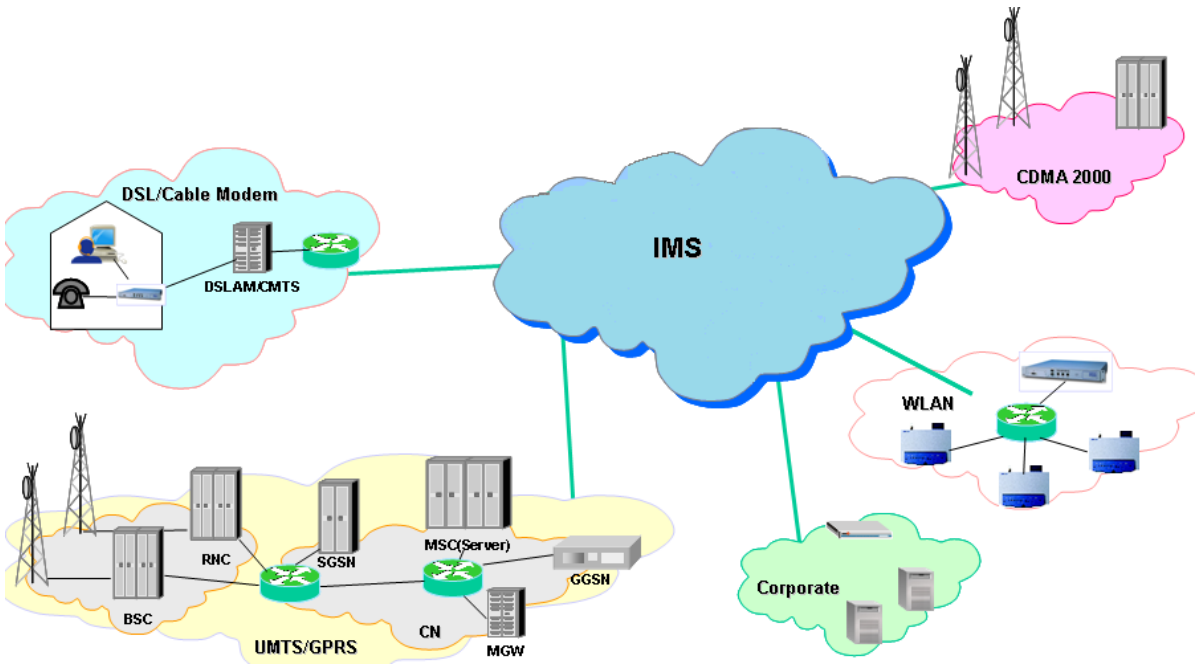

Figura 15. Ejemplo de múltiples redes de acceso conectadas a la red troncal multimedia

3.2. Características principales de IMS.

Las características más relevantes de la red multimedia IP son:

3.2.1. Sesiones multimedia IP

El concepto principal es que los usuarios de la red establezcan una única sesión de comunicación con la red y durante la misma pueda hacer uso de todos los servicios a los que estén suscritos sin tener que establecer sesiones de comunicación adicionales, con libertad para empezar a utilizar los servicios o dejar de usarlos en cualquier momento de la sesión en curso.

La red multimedia para el soporte del establecimiento, modificación y eliminación de sesiones multimedia utiliza como protocolo de señalización principal el protocolo de nivel de aplicación SIP (Session Initiation Protocol) del IETF [19]. Este protocolo de texto plano cliente-servidor, definido para la gestión de sesiones en un entorno no orientado a la conexión requería algunas funcionalidades añadidas para convertirse en el protocolo indicado para el control en la plataforma multimedia. El IETF resolvió algunas de las carencias de la especificación inicial con la definición de extensiones posteriores y cabeceras adicionales (definiciones en lo relativo a la compresión, negociación de precondiciones, seguridad y otros) que permite que el protocolo SIP sea el protocolo encargado del control y la gestión de la señalización de las sesiones multimedia, de la identificación de elementos y de usuarios, y del control y gestión de los servicios.

El protocolo SIP es un protocolo flexible y muy potente que permite incluir contenido MIME en el cuerpo de los mensajes SIP. Esta característica permite que en los mensajes SIP se transfieran mensajes SDP (Session Description Protocol) [20] que tiene como función describir las características en las que se establece una sesión multimedia. A través de los mensajes SDP contenido en los mensajes SIP, los usuarios de la red multimedia negocian el tipo de comunicación que desean establecer e indican las capacidades de que disponen para cumplirla. Los extremos indican los medios que desean utilizar para comunicarse con el otro extremo, las codificaciones soportadas por cada terminal para satisfacer dichos flujos de medios, los requerimientos de ancho de banda y por tanto de calidad de servicio deseados y soportados por cada extremo. La principal novedad en este aspecto es que la red multimedia no realiza la asignación estática de recursos sino que permitirá que los extremos de la comunicación, ya sean usuarios o servicios, elijan los medios, ancho de banda o calidad de servicio que desean utilizar en la comunicación de manera negociada y dinámica entre ellos y la red simplemente se encargará de verificar que dichas condiciones están dentro de las políticas del operador, de los servicios permitidos por los perfiles de los usuarios y de las recursos disponibles por la red [21].

3.2.2. Conectividad IP

Una capacidad imprescindible que tienen que disponer los equipos de usuario, UE, es que dichas sesiones se establezcan sobre una conexión IP. Dicha conectividad entre otras cosas permite el desarrollo de una red troncal de transporte a través de un estructura eficiente de transporte IP que soporta tanto el trafico de señalización como el tráfico de usuario y e interconecta todos los servicios con todas las redes de acceso al mismo tiempo convirtiéndose en una plataforma multiacceso y multiservicio.

En un primer momento se determino el uso de la nueva versión del protocolo de Internet IPv6 para el desarrollo de la plataforma debido a la capacidad casi ilimitada de

direccionamiento que ofrece, las mejoras en cuanto a seguridad y calidad incorporadas y una mayor simplicidad en el transporte de los datagramas IP [18] pero debido a lento despliegue de esta nueva versión del protocolo IP, finalmente se ha optado también por incluir compatibilidad hacia la versión anterior, IPv4, que aunque se encuentra en los límites de direccionamiento posible, se encuentra en su máximo nivel de despliegue en los diferentes equipos de las actuales redes de conmutación de paquetes (routers, switches, firewalls, etc.) facilitando la rápida integración y la interoperabilidad de la nueva infraestructura con los dominios de red existentes [21].

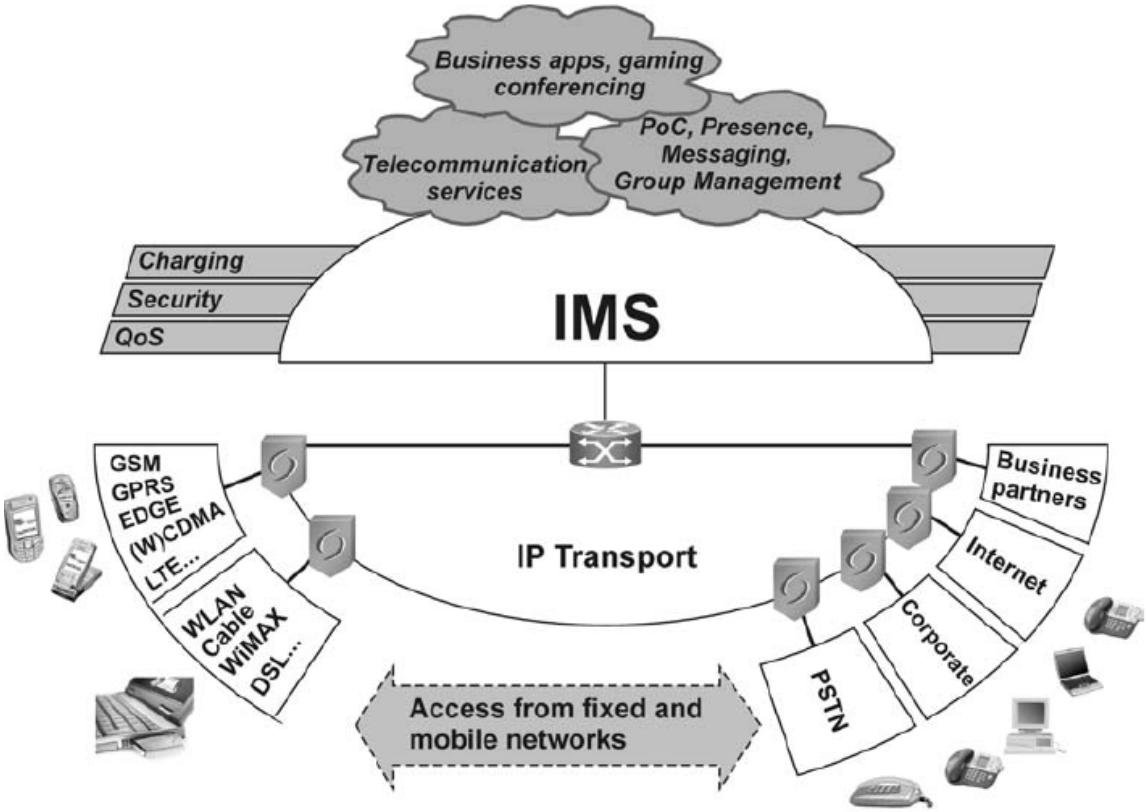

Figura 16. Red de transporte IP común a todas las redes de acceso. Servicios independientes de los tipos de accesos a la red.

3.2.3. Calidad de servicio

Es uno de los aspectos clave en el desarrollo de IMS, puesto que permite establecer una sesión multimedia con un nivel de calidad de servicio asegurado, lo que se traduce en trasladar la experiencia de usuario propia de las redes de comunicaciones convencionales a la red de conectividad IP.

En el momento de establecer o modificar una sesión, el equipo de usuario negociará las condiciones en las cuales se realizará, expresando sus capacidades e indicando cuáles son sus requerimientos de calidad del servicio. Posterior a la negociación de los parámetros de calidad el UE reserva los recursos adecuados en la red de acceso.

Cuando las condiciones de QoS extremo a extremo se cumplen, el equipo de usuario realiza la codificación y el empaquetamiento de la información con los

protocolos acordados y los envía a las redes de acceso y transporte. El operador por su parte se encarga de asegurar el cumplimiento de las condiciones de calidad de servicio en la red. La red multimedia es por tanto el responsable último de proporcionar y gestionar la infraestructura básica que garantizará los niveles de calidad necesarios para cada servicio a través de asignación y reserva de recursos en los niveles de transporte (nivel de transporte en la red de acceso).

La red multimedia permite la aplicación de diferentes niveles de calidad de servicio en función de diferentes consideraciones como el tipo de servicio solicitado, el perfil de los usuarios involucrados, la red de acceso, etc. adaptando las características de la sesión a la circunstancias en la que se desea establecer la comunicación y permitiendo un uso flexible y adaptativo de los recursos disponibles.

3.2.4. Seguridad.

La seguridad es un elemento fundamental en las redes de telecomunicaciones. Podemos dividirla entre los mecanismos de seguridad utilizados dentro de la red y la arquitectura de seguridad de la red multimedia.

3.2.4.1. Mecanismos de autenticación, autorización y registro (AAA)

IMS describe un conjunto de mecanismos de autenticación, autorización y registro (AAA) necesarios para realizar las funciones de protección y control de acceso a la red por parte del UE así como funcionalidades de integridad y de confidencialidad.

Antes de poder acceder a los servicios de la red, ésta y el equipo del usuario tienen que estar autenticados entre sí (entidades validadas y reconocidas mutuamente y verificadas como auténticas), y la red tiene que autorizar al usuario para poder acceder los servicios de la red y registrar y controlar el uso de los recursos asignados al mismo. Además de los métodos mencionados las funcionalidades de integridad y confidencialidad son obligatorias.

3.2.4.2. Arquitectura de seguridad

La arquitectura de seguridad de la red estará compuesta por varios elementos [21]:

- Seguridad del dominio de red (NDS en sus siglas en inglés) que tiene como función proporcionar seguridad a nivel de red entre elementos de un mismo dominio y seguridad entre diferentes dominios de red.
- Seguridad de acceso, que define los mecanismos de seguridad para acceder a la red.
- Y una arquitectura genérica de autenticación que proporciona una estructura para la autenticación y ayuda al nivel de seguridad de acceso a facilitar el acceso a los servicios.

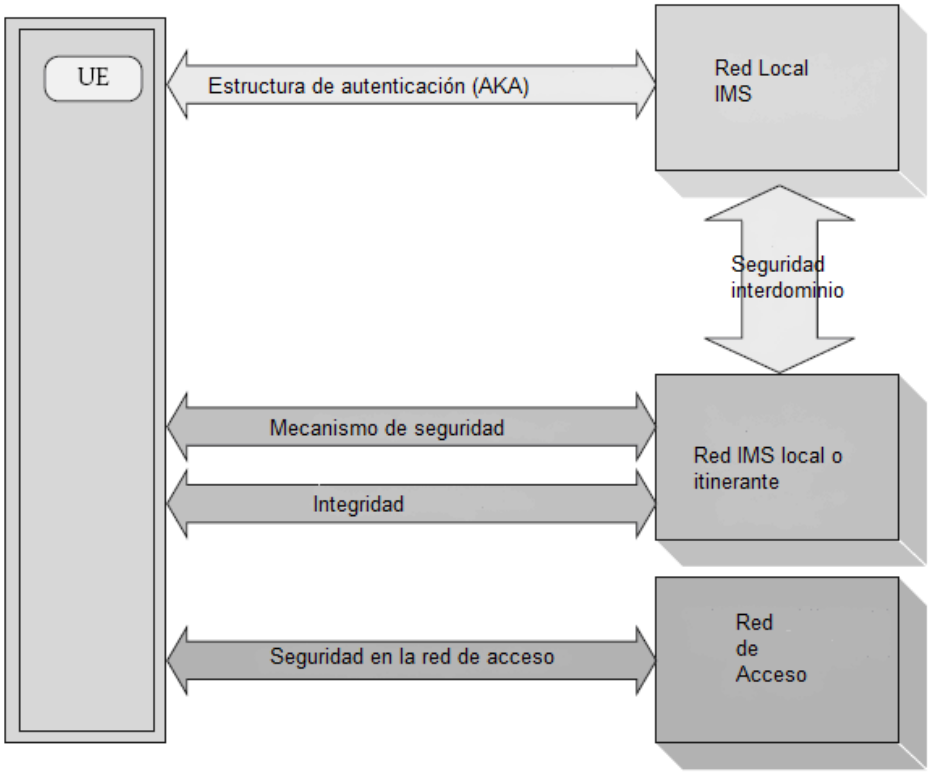

Figura 17. Niveles de seguridad entre cada nivel de red.

3.2.4.3. Seguridad del dominio de red (NDS)

Concepto de seguridad que se encarga de la protección de todo el tráfico IP que se transmite a través del nivel de transporte de la red troncal.

Un dominio de seguridad es una red o parte de una red que esta operada por un único operador o autoridad que mantiene una política de seguridad uniforme dentro de todo el dominio. Esta división habitualmente coincide más o menos con la red troncal de un operador de red. Los extremos entre dominios de seguridad están protegidos por entidades de acceso de seguridad (SEG en inglés) que se encargan de interconectar los diferentes dominios de seguridad entre sí. El intercambio de tráfico entre diferentes dominios de seguridad se realiza asegurando las funciones de autenticación, confidencialidad e integridad con combinación de mecanismos de seguridad en los datos (criptografía) y mecanismos de securización de protocolo en el nivel de red (IPsec) [21].

3.2.4.3.1. Puertas de acceso o pasarelas de seguridad (SEGs)

Son las entidades de seguridad situadas en los extremos del dominio y son los responsable de ejecutar la política de seguridad al tráfico de entrada y de salida que atraviesa el dominio de seguridad y de interconectarse con las pasarelas de seguridad de otros dominios. Estas entidades pueden actuar como firewalls para impedir ciertos tipos de acceso y filtrado de tráfico para evitar el paso de ciertas clases de tráfico al dominio.

3.2.4.3.2. Distribución y gestión de claves entre dominios de seguridad

Cada puerta de acceso (SEG) negocia, establece y mantiene asociaciones de seguridad IPsec (IPsec SA en inglés) con los dominios con los que se interconecta [22]. Estas asociaciones de seguridad, que son conexiones seguras entre dominios, están desarrolladas sobre el protocolo IKE para la distribución y la gestión de claves de seguridad y sobre el protocolo de seguridad ESP para mantener la encriptación (algoritmo 3DES), integridad de los datos y autenticación del origen de datos (MD5 y SHA-1) .

Los puntos de acceso de seguridad (SEGs) son los únicos elementos que se comunican con otros dominios. Estas entidades normalmente establecen un túnel IPsec activo en cada momento con cada par con el que se comunican y sobre este túnel es sobre el que se establece la conexión (ESP IPsec SA), es decir el datagrama IP securizado se encapsula dentro de un paquete ESP para el envío entre dominios [22].

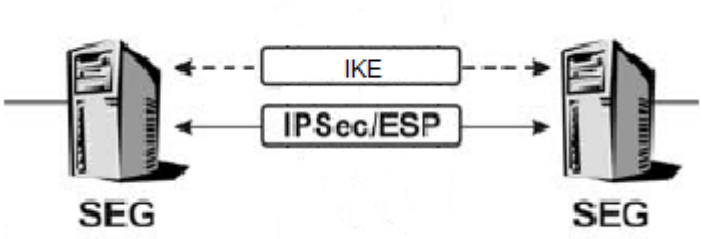

Figura 18. Conexiones de seguridad establecidas entre dos extremos de dominios de seguridad

3.2.4.4. Seguridad en el acceso a la red

La seguridad de acceso se encarga de proteger la señalización intercambiada entre el terminal de usuario y el punto de entrada a la red multimedia para ese usuario, proporcionando los mecanismos, algoritmos y claves necesarias para esta función. Para securizar el acceso se debe proporcionar autenticación, para que el terminal y la red se validen como auténticos y autorizados, integridad de datos, encriptación y privacidad.

Todas estas funciones se realizan a través de un acuerdo de seguridad y autenticación basado en el protocolo AKA (Authentication Key Agreement). El transporte de los parámetros de seguridad que se emplearán en las comunicaciones entre el terminal del usuario y la red se realizan sobre la propia estructura del protocolo de comunicación SIP, integrando en las cabeceras del protocolo la información de seguridad y al igual que entre dominios de red, estableciendo asociaciones seguras IPsec para proporcionar las facilidades de encriptación e integridad de datos. Ambos protocolos incorporan del conjunto de claves para la sesión generadas por el mecanismo AKA [21].

3.2.4.4.1. Protocolo de Autenticación (AKA)

El protocolo para la autenticación tanto del terminal de usuario como de la red de forma automática, es decir, sin intervención del usuario, es el protocolo AKA. A partir de una clave compartida (K) y unos algoritmos comunes almacenados tanto en el extremo del usuario como en la red se generan un conjunto de resultados que servirán para que ambos extremos verifiquen su autenticidad y se validen entre sí.

El procedimiento funciona como se detalla, la red genera un código de aleatoria (RAND) y una prueba de autenticidad (AUTN) para preguntar al terminal. Éste utiliza este último parámetro para verificar la identidad de la red. Para responder el modulo del usuario (ISIM) genera una respuesta (RES) a partir de la clave almacenada en su interior (K) y con el código recibido (RAND). La respuesta generada (RES) es comparada por la red con la respuesta esperada por la red (XRES) para verificar la autenticidad del usuario. Si coinciden se produce la autenticación entre ambas partes y como resultado se generan un par de claves de sesión: Una clave de encriptación (CK) y una clave de integridad (IK) que serán usadas en las comunicaciones posteriores entre ambas partes. Además de todo lo mencionado durante el proceso de autenticación ambas partes utilizan un mecanismo de control de secuencia (SQN) para indicar en qué numero de secuencia se encuentra el proceso y mantener la sincronización entre extremos. Si alguna de las dos partes proporciona un número de secuencia diferente del esperado por el otro extremo, el proceso de autenticación se interrumpe y se envía un fallo de sincronización indicando el problema al extremo opuesto [24].

3.2.4.5. Otros esquemas de seguridad y autenticación

El método de seguridad expuesto anteriormente (AKA IPsec ESP SA) se trata de la solución completa de seguridad para las redes de acceso de las especificaciones de acceso móvil (3GPP) [22, 23 y 24]. Sin embargo esto no implica que todas las redes de acceso (red de acceso fijo (TISPAN), red de acceso inalámbrico (WiMax, WLAN), red de acceso de cable o fibra (CableLabs)) permitan autenticar y autorizar a la red multimedia con el mecanismo de seguridad anterior. Las posibles alternativas en el esquema de seguridad y autenticación son los siguientes:

- SIP Digest sobre TLS
- GPRS-IMS Bundled Authentication (GIBA), Autenticación de GPRS-IMS
- NASS-IMS-bundled authentication (NBA), Autenticación de NASS-IMS
- Autenticación de elemento verificado (TNA en sus siglas en inglés)

Cada uno de estos esquemas es utilizado para unos casos concretos que detallaremos a continuación.

3.2.4.5.1. SIP Digest sobre TLS

Es el método de seguridad nativo de SIP basado en el mecanismo HTTP Digest [38 y 39] donde el usuario y la red comparten una contraseña o clave preestablecida y asociada con la identidad privada de usuario (IMPI) que es la que autentica al suscriptor. Cuando se solicita acceso a la red por parte del UE, la red pide al usuario de usuario que facilite esta credencial y se compara con la contraseña almacenada en la red para su verificación [21 y 24]. Para evitar riesgos para la seguridad, el usuario puede probar que conoce la clave compartida sin necesidad de enviar ésta a través de la red en lo que se conoce como mecanismo de acceso compartido, en nuestro caso a través de la estructura del protocolo SIP, en lo que se conoce como SIP Digest [18]. Estos mecanismos utilizan una función o algoritmo de un solo sentido que utiliza un conjunto de datos como argumentos (en este caso la identidad IMPI y clave compartida entre otros) y en los que es computacionalmente imposible obtener los argumentos a partir del resultado [38].

El uso de este esquema de seguridad está destinado a redes de acceso diferentes a las redes definidas en las especificaciones de 3GPP donde el terminal de usuario no soporta el mecanismo de autenticación y autorización IMS-AKA IPsec y por lo tanto se requiere el uso de otra tecnologías de seguridad.

Para cubrir las funciones de protección de confidencialidad y de integridad se requiere el uso de otro mecanismo conocido como TLS, que es un protocolo que opera sobre un nivel de transporte orientado a la conexión (TCP) que permite que el usuario y la red establezcan una conexión segura a partir de la negociación de un algoritmo criptográfico común para cifrar el tráfico enviado y del intercambio de claves públicas y certificados digitales de autenticidad (CA) entre ambos extremos para conseguir una comunicación integra y confidencial [18].

3.2.4.5.2. NASS-IMS-bundled authentication

Este esquema de autenticación describe el mecanismo de seguridad seguido para aquellos equipos de usuario que acceden a la red multimedia a través de redes de comunicaciones fijas o cableadas (xDSLs, WAN, redes corporativas PBX, etc.) y definido por el subsistema de acceso de la propia red NASS, en su acrónimo en inglés, establecido por el ETSI TISPAN en la adaptación relativa de la red multimedia IP de 3GPP para su interconexión con redes fijas o cableadas [21]. El subsistema de acceso a la red NASS, dispondrá de sus propios mecanismos de seguridad y autenticación en los cuales la red multimedia confiará para permitir la autenticación del usuario dentro de la red IMS.

Para poder usar esta forma de conexión se deben cumplir unas condiciones muy concretas:

- La red de acceso proporcionará los medios al nivel multimedia para asegurar que el usuario se encuentra conectado desde una

localización fija. Los conceptos de movilidad y roaming (itinerancia) no estarán permitidos por la red de acceso.
- La red de acceso deberá asegurar la confidencialidad y la integridad de la comunicación.
- La red de acceso proporcionará medidas anti-suplantación de dirección de red (IP).

El punto de conexión a la red IMS para este usuario realizará el control de estas condiciones estableciendo una relación entre la dirección IP del usuario (desde la que se recibe la petición) y la información de localización que facilita la red de acceso.

3.2.4.5.3. GPRS-IMS-Bundled Authentication (GIBA)

Este mecanismo de seguridad y autenticación desarrollado para las primeras fases de implantación de la red multimedia, que no disponen de una infraestructura de seguridad definitiva y se basan en los mecanismos de seguridad del nivel subyacente de datos, en este caso, GPRS. Esta ausencia de un modelo de seguridad completo es debida en parte a que los terminales de usuario en muchos casos todavía no soportan los métodos de seguridad establecidos para IMS. En ésta situación, este mecanismo de seguridad proporciona un nivel suficiente de protección contra las amenazas más importantes que aparecen en las primeras implementaciones de IMS sin dejar de ser una solución interina que facilita la compatibilidad y la migración con las soluciones definitivas de seguridad proporcionadas para IMS (AKA IPsec/ SIP Digest TLS) y minimiza el posible impacto sobre los dispositivos para que la interoperabilidad con los UE sea la mejor posible.

El funcionamiento de este mecanismo se basa en que la red multimedia establece una relación de seguridad a partir del vínculo de la identidad privada/pública del usuario almacenada en la red y la dirección IP reservada para el equipo de usuario por el nivel de GPRS. El contexto PDP establecido por el GGSN de la red de datos GPRS determina cual es la dirección IP asignada al usuario, su MSISDN y su IMSI y se los facilita a la red multimedia para que ésta, establezca una relación univoca con las identidades publicas y privada del suscriptor. Si se produce cualquier modificación o cancelación en los parámetros GPRS proporcionados a la red, ésta es notificada a la red multimedia para que realice las acciones oportunas. Este mecanismo tiene como fin que el usuario sólo pueda acceder a los servicios de la red multimedia a través de una única dirección IP de red (la que está asociada con la identidad privada de usuario) [21].

3.2.4.5.4. Trusted Node Authentication (TNA)

El objetivo de este método es facilitar acceso seguro a la red a través de un elemento de red verificado que se interconecta con la red multimedia. El principal caso donde esto se produce cuando se interconecta hacia redes del dominio de circuitos conmutados. Este elemento de interconexión se encontrará verificado por la red multimedia como seguro y proporcionará suficientes

medios para realizar el proceso de seguridad y autenticación en el dominio de circuitos conmutados, Ej.: Mobile Switching Center de una red móvil terrestre conectado a través de la interfaz ICS a la red multimedia.

3.2.5. Facturación y tarificación

La tarificación en la red multimedia se basa en el registro de toda la información relevante de una sesión por parte de los elementos de control. El registro de los usuarios implicados, servicios utilizados, permisos y autorizaciones recibidas y los asocia con los registros de uso que recibe de la red de acceso donde se transfieren los flujos de datos y de señalización. De esta manera la red multimedia tarifica en función de la duración, contenidos, destinos, servicios utilizados, volúmenes de datos o cualquier combinación de éstos, creando un sistema de tarificación eficiente y diferenciado por servicio y por uso para aplicar un modelo de facturación más flexible, independiente y eficiente. Flexible puesto que permite que cada suscriptor pueda ser facturado por el conjunto de servicios específicos utilizados de manera que cada suscriptor tenga su propio esquema de facturación. Eficiente puesto que el modelo de registros de llamadas o sesiones (CDRs) se integra fácilmente en los actuales modelos de facturación y no requiere grandes adaptaciones, e independiente puesto que los sistemas de facturación dentro de la red multimedia se encuentran completamente separados de las funciones principales de la red de tal manera que estos son también independientes del nivel de aplicación y no están ligados a los servicios disponibles, sin interferir con el principio de escalabilidad de la red.

3.2.6. Movilidad y Roaming

Para cualquier usuario la posibilidad de obtener conexión a la red y acceso a los servicios independientemente de su posición geográfica es un requisito fundamental. Existen diversos modelos para la gestión de la conexión, en los casos donde el usuario se encuentra fuera de la zona de servicio de su operador, donde o la conexión es gestionada desde la red en itinerancia (red visitada) o desde la propia red local. La primera de las dos posibilidades permite que la gestión de los recursos de los medios se haga en la red en itinerancia y esto se traduce en una mayor eficiencia en la gestión de los mismos [21]. La segunda posibilidad sin embargo permitiría que un usuario pueda acceder a los servicios de la red IMS aun en el caso de que la red a la que esté conectada solo proporcione conectividad IP básica, por ejemplo un usuario que está conectado al servicio GPRS de la red visitada pero los servicios son proporcionados por la red multimedia del usuario.

La gestión de la movilidad o la conectividad desde diferentes puntos geográficos pertenece a las funciones propias de las redes de acceso aunque la red troncal realiza un papel fundamental al almacenar la información de localización del terminal en las bases de datos principales de la red junto con el resto de la información de usuario puesto que esta información es relevante durante diferente procesos que tendrán lugar en la propia red multimedia (asignación de servidor de control durante el registro de usuario, comunicación iniciada por un servicio hacia un usuario determinado, etc.)

Estas características solo serán de aplicación en redes de acceso móvil o donde los terminales de acceso dispongan de movilidad para conectar a diferentes puntos de acceso.

3.2.7. Interconexión con las redes existentes y tránsito

IMS tiene que tener la capacidad de interconectarse con todas las redes troncales actuales para que los usuarios puedan interoperar con abonados de otros dominios u operadores sin importar del tipo que sean. Para esta tarea es necesario la capacidad de interconectarse con:

- Redes de circuitos conmutados existentes (PSTN, ISDN y dominio de circuitos de PLMNs), basadas en SS7.
- Redes de conmutación de paquetes (Internet, dominio de conmutación de paquetes de PLMN (GPRS), redes corporativas y privadas, redes inalámbricas de datos.)
- Redes multimedia de otros operadores.

La red tiene que ser capaz de determinar a qué dominio y a que red pertenece el usuario de destino durante el establecimiento de una sesión y entregar la señalización a los elementos encargados de realizar la interconexión y la conversión tanto de medios como de señalización con la red de destino de manera que sea un proceso completamente transparente para los usuarios finales. La interconexión se debe producir en ambos planos, puesto que en algunos casos, como las redes de conmutación de circuitos utilizan protocolos diferentes tanto para señalización como para los medios y ambos niveles tienen que ser adaptados para una correcta interoperabilidad.

Otra de las funciones de interconectarse con las redes existentes es realizar operaciones de tránsito, ya que una red no puede estar interconectada con todas las redes del mundo, la solución pasa por enviar trafico a través de una o varias redes de tránsito que facilitan la conexión hasta la red de destino. El comportamiento de la red en este caso es bastante sencillo, una vez que recibe una petición de conexión analiza la dirección del destinatario y en base a una búsqueda interna (resolución DNS/ENUM, consulta a base de datos interna o cualquier otro método) decide en que dominio entregar la solicitud. Esta funcionalidad le confiere una versatilidad importante al realizar funciones de tránsito para diferentes escenarios (transito para clientes propios que no pertenezcan a IMS, tránsito para otros operadores de redes multimedia o de redes existentes (PSTN, PLMN….), proveedor para redes corporativas etc.)

3.2.8. Servicios e integración

El objetivo principal de las redes IP multimedia es desde la perspectiva del proveedor disponer de una red de comunicación que aporte un alto valor añadido en el desarrollo de un nuevo concepto de servicios centrados en el usuario que permita la combinación flexible e innovadora de las características que darán una experiencia de usuario completa y personalizada basada en las elecciones y preferencias de cada suscriptor.

Para el desarrollo de esta característica y la independencia del nivel de aplicación o servicio se introduce el concepto de habilitadores de servicio o habilitadores multimedia. Estos habilitadores tiene por función ser utilizados en el desarrollo, despliegue y operación de un servicio para de una forma simplificada y estandarizada permitir la creación y la interconexión de nuevos servicios desarrollados por el operador

o por un tercero [21]. Estos habilitadores proporcionan las capacidades fundamentales que aseguran la interoperabilidad de todos los elementos de la red entre sí, dispositivos, operadores y proveedores de servicio interactuando tanto con el nivel de servicio como con la arquitectura de red subyacente. Estos habilitadores así mismo permiten reducir los costes de desarrollo de nuevos servicios a los desarrolladores mejorando la eficiencia de las inversiones en nuevas funcionalidades y optimizando los procesos de despliegue.

El uso de estos elementos que engloban capacidades básicas que se reutilizan con múltiples servicios tiene también como función asegurar que todas las funciones de servicio añadidas al nivel de aplicación son consistentes con el concepto de experiencia de usuario integrada (por ejemplo , no se incorporaran servicios a través de habilitadores que compartan las mismas funcionalidades básicas, para que no se repitan procesos como que un mismo usuario tenga que introducir sus credenciales para acceder a un servicio concreto una vez que tiene una sesión multimedia iniciada).

Por otro lado IMS define componentes de pasarela que interactúan con las plataformas de creación de servicios existentes de otras redes, como los entornos OSA y CAMEL utilizados en el desarrollo de servicios para las redes móviles 2G y 3G. Esta facilidad añade más versatilidad a la red puesto que permite que los desarrolladores reutilicen estructuras de desarrollo ya conocidas para nuevos servicios e incluso se aprovechen los servicios ya existentes para la nueva plataforma multimedia.

3.2.9. Identificación

Una de las posibilidades más interesantes que permiten las redes de nueva generación es la posibilidad de que un mismo usuario que disponga de varios dispositivos pueda registrar la misma identidad pública de usuario en múltiples equipos. Para ello se desarrollan un conjunto de conceptos de identificaciones.

3.2.9.1. Identidades privadas de usuario

Es una identidad global y única definida por el operador que es utilizado exclusivamente para la autenticación, administración y registro de una suscripción de usuario dentro de la red local y tiene como función identificar la información de usuario almacenada en la red. En relación a esta información privada:

- Se incluirá dicha identificación dentro de cada petición de registro desde el UE hacia la red.
- Solo será usada y autenticada durante el proceso de registro, re-registro y desregistro del usuario en la red.
- Esta identidad no es utilizada con propósitos de enrutamiento.
- La identidad deberá permanecer asociada a un usuario durante todo el tiempo de vida de la suscripción y almacenada de una forma segura en la ISIM (si el terminal de usuario dispone de ella). Además dicha identidad no puede ser modificada por el usuario en ningún caso.

Ejemplo de identidad privada: usuario1@home1.operador.net

3.2.9.2. Identidades públicas de usuario

Las identidades públicas de usuario, son aquellas identidades que permiten identificar a un usuario y solicitar sesiones con otros usuarios y donde el usuario puede ser localizado. Estas entidades pueden tener dos formatos, formato de telecomunicaciones, TEL URL, con el formato universal E.164 (Ej.: +123456789) o formato de nombres de Internet, SIP URI (Ej.: sip:user@domain). Estas identidades tienen que cumplir algunas reglas generales de funcionamiento:

- Al menos una identidad pública de usuario tiene que está registrada para poder establecer sesiones de comunicación con otros usuarios.
- Al menos una identidad pública tiene que estar almacenada en el modulo de identidad de servicios multimedia (ISIM, similar a las tarjetas SIM en las redes móviles actuales). Y esta no puede ser modificada en ningún caso por el usuario.
- Estas identidades no son autenticadas por la red durante el proceso de registro en la misma.
- Es posible registrar múltiples identidades públicas en cada proceso de registro en la red. Se pueden agrupar varias identidades públicas en un único subconjunto que permite el registro implícito de todas las identidades que pertenecen a dicho grupo cuando al menos una identidad del mismo ha sido registrada explícitamente.
-

3.2.9.3. Relación de identidades públicas y privadas de usuario.

Como se muestra a continuación la relación entre identidades públicas y privadas puede ser de diversas formas puesto que solo existe una suscripción del usuario en la red, pero esta puede estar formada por varios equipos cada uno con su identidad privada de usuario y su identificador de equipo que están conectados a la misma identidad pública o a diferentes identidades como se indica en la siguiente figura.

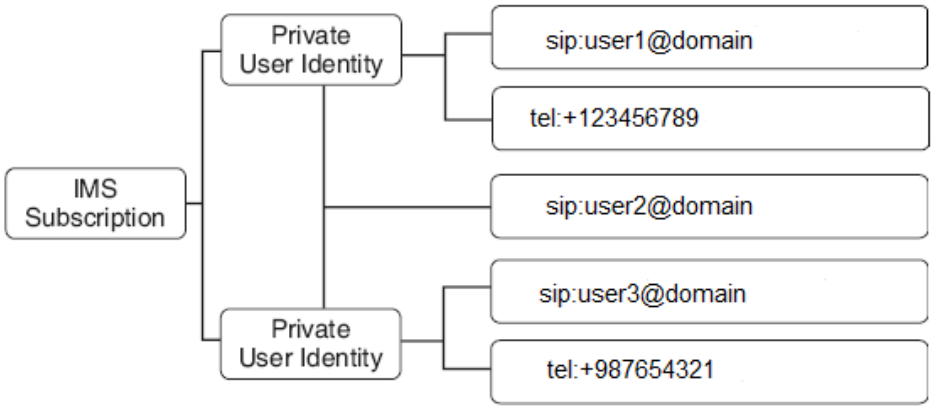

Figura 19. Relación entre identidades públicas y privadas.

3.2.9.4. Identidades globales

Debido a que varios dispositivos pueden compartir una misma identidad de usuario al mismo tiempo es necesario definir un nuevo mecanismo que permita identificar un solo dispositivo cuando varios equipos compartan una identidad. Este identificador (GRUU en inglés) es el que identifica cada combinación de identidad pública de usuario e identidad de equipamiento lo que permitirá dirigir peticiones a un único equipo entre varios como se ve en la figura 8. Los hay de dos tipos:

- P-GRUU: Es un identificador invariable que se genera para la combinación de la identidad pública y el identificador del dispositivo físico donde se registra dicha identidad y que dura durante toda la existencia de la combinación.

- T-GRUU: Es una identidad de duración determinada que se genera con cada registro del usuario en la red y que mantiene la identidad pública del usuario oculta.

Cada vez que una identidad publica se registra en la red, se genera un par de identificadores globales (un P-GRUU y un T-GRUU) para cada UE registrado con dicha identidad pública.
La red será capaz de obtener la identidad pública de usuario directamente del identificador P-GRUU si fuera necesario y enrutará las peticiones dirigidas a un GRUU al terminal de usuario registrado con ese GRUU.

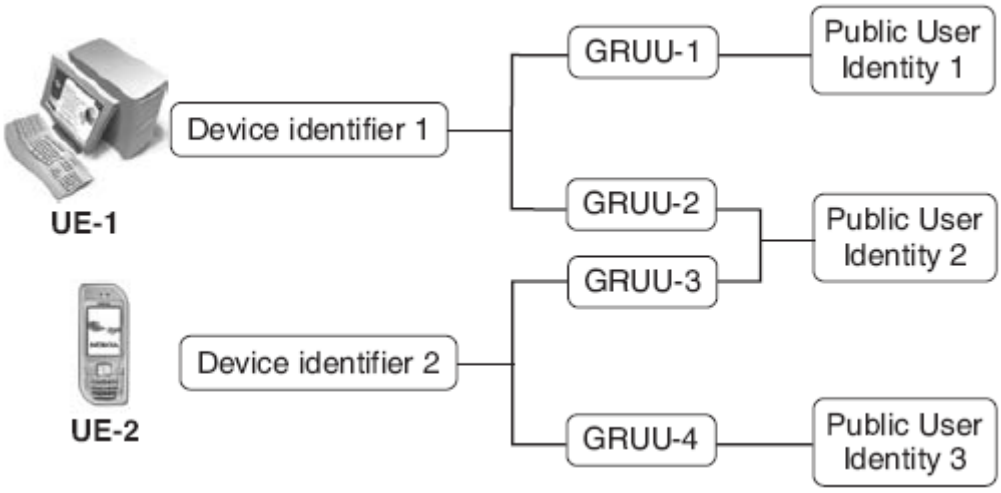

Figura 20. Relaciones entre identidades de usuario e identificadores de dispositivos a través de GRUUs

3.2.9.5. Identidades de red e identidades de servicio

Al igual que los usuarios, los servicios ofrecidos por el nivel de servicio disponen de un sistema de identificación, conocido como identidades de públicas

de servicio (PSI en inglés). La llamada por parte de un usuario de la red de una identidad pública de servicio producirá la ejecución de la lógica del servicio en el servidor de aplicación donde se aloja dicha función.

Por otro lado los elementos de red también serán identificados y accesibles usando un SIP URI (nombre del Host o dirección de red) válido que permitirá la comunicación entre nodos y de estos con los equipos de los usuarios.

3.2.10. Perfil de Usuario y Servicio

Un perfil de usuario es un conjunto de información relativa a un subscriptor que es almacenada en las bases de datos de la red. El operador asigna un perfil de usuario cuando el usuario establece una suscripción con el operador el cual contiene al menos una identidad privada del usuario (que identifica y autentica al usuario durante el registro) y uno o más perfil de servicio, que es un conjunto de información relativa a los servicios del usuario, preferencias del usuario y otros. El perfil de servicio está compuesto de cuatro tipos de información, detallados a continuación.

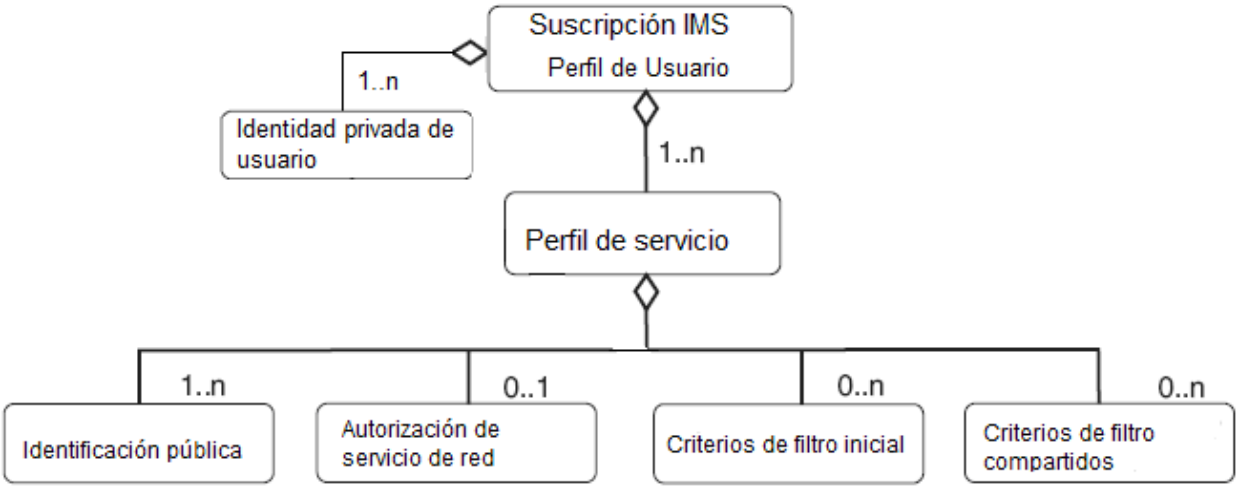

Figura 21. Perfil de usuario y de servicio

3.2.10.1. Identificación publica

Este campo contiene una o más identidades públicas de usuario o de servicio sobre las que se aplica el perfil de servicio en cuestión.

3.2.10.2. Autorización de servicios de red

Un identificador del tipo de perfil servicio que indicara el nivel de servicio que tiene dicho suscriptor y que permite que la red defina diferentes clases de clientes con diferentes capacidades. Incluye también un identificador

de de servicio que es una lista de identificadores de los diferentes servicios disponibles.

3.2.10.3. Activación de servicio o Criterios de filtrado inicial

Cuya función principal es determinar si se cumplen las condiciones para enviar una petición de servicio al servidor de aplicación que almacena el servicio. El criterio de filtrado inicial está compuesto por varios campos.

- El primero es una prioridad que marcará el orden en el que el filtro será evaluado dentro del perfil del servicio.

- Uno o varios puntos de activación, que son las condiciones que deben ser cumplidas para que la petición sea enviada al servidor. Estas condiciones son un conjunto de valores concretos para uno o varios campos de una petición SIP, que combinados conforman la condición de punto de servicio completa.

- Información del servidor, donde se indica la dirección SIP URI del servidor de aplicación (AS) que tiene que ser contactado en caso de que se cumplan las condiciones así como información de de operación para el elemento de control de la sesión en caso de que este servidor no responda.

- También se puede incluir información opcional de utilidad para el servidor de servicio en cuestión.

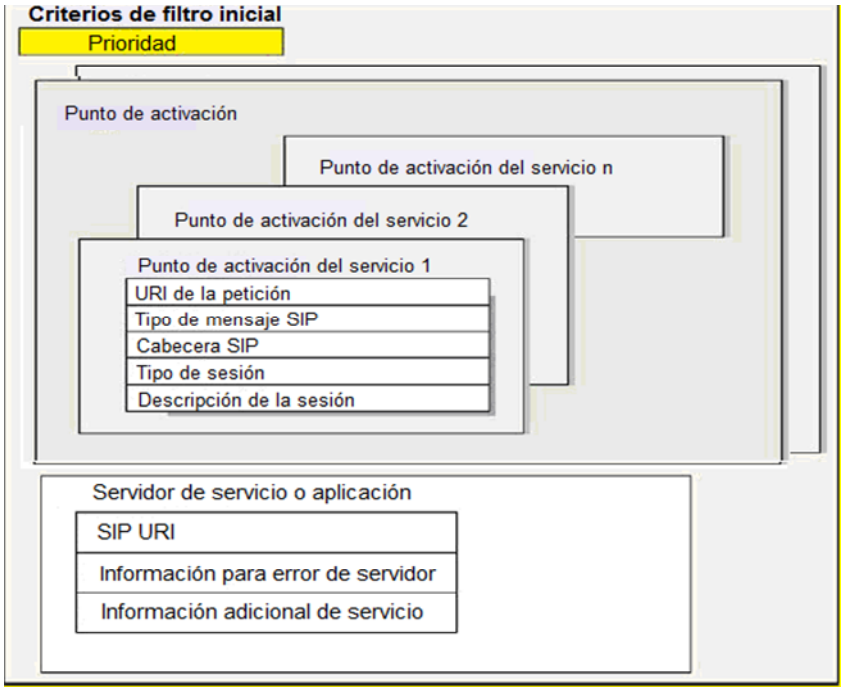

Figura 22. Estructura de un criterio de filtrado inicial

3.2.11. Sesiones de emergencia

La red multimedia incorpora una funcionalidad que permita detectar llamadas o sesiones de emergencia y realizar el apropiado tratamiento y enrutamiento hacia el centro de emergencias más conveniente según los datos de localización disponibles por el operador de red y el tipo de emergencia requerida. Esta funcionalidad específica requiere entidades funcionales o elementos especialmente dedicados a estas tareas, encargados de obtener y verificar la información de localización del usuario de la forma más precisa posible y de clasificar el tipo de emergencia. Si la información disponible no es del todo fiable, esta entidad de control se apoya en una función de información de localización, disponible en algunas redes, donde existe más de una base de datos para el almacenamiento de la información de usuario.

Los servicios de emergencia proporcionados por la red deberán ser independientes de la red de acceso y la tecnología de acceso que utilice el terminal de usuario. El sistema deberá ser capaz de diferenciar y discriminar entre sesiones de emergencia y sesiones que no lo son, lo que permitirá que las primeras reciban un tratamiento especial, en lo relativo a disponibilidad del servicio, prioridad, enrutamiento preferente, calidad del servicio y todas aquellas funciones que puedan ser relevantes en la sesiones de emergencia.

El proceso para poder establecer una sesión de emergencia comienza por el registro de emergencia. Si el equipamiento de usuario (UE) no se encuentra en la red local (roaming) o no esta registrado en la red en ese momento, la red requerirá que el usuario realice el registro de emergencia. El registro de emergencia sigue el procedimiento habitual de registro de usuario con la diferencia que en ésta situación no está permitido que se desregistre el terminal de la red. Este procedimiento es completamente independiente del registro normal del resto de usuarios.

El equipo de usuario podrá dar a conocer a la red que se solicita el establecimiento de una sesión de emergencia marcando el numero de un centro de emergencia y el terminal podrá enviar directamente el numero marcado (en casos de roaming fuera de la red local) o traducir dicho numero por un nombre de recurso (URN en sus siglas en inglés con formato urn:service:sos) por lo tanto la red soportará tanto números de emergencias en formato TEL URI como SIP URI. El elemento de la red encargado de gestionar todas las conexiones para ese UE comprobará este identificador o numero con una lista de servicios locales de emergencia configurados en la red para elegir el nodo de gestión de sesión de emergencia más adecuado. Este a su vez realizará la selección del centro de emergencia apropiado al que enrutará la llamada de emergencia. En el caso particular de que el usuario no se encuentre localizado en la red local, el escenario habitual es que la red visitada o en itinerancia se encargue del establecimiento de la sesión de emergencia.

3.2.12. Compresión

La señalización de control de las sesiones multimedia en la red, se realizan por medio del protocolo de señalización en texto plano SIP, que proporciona una estructura flexible para que se puedan establecer sesiones multimedia bajo condiciones negociadas. Debido a que el proceso de señalización en la red es largo y complejo

puesto que se requiere la negociación de las condiciones, incluidos los medios a usar para cada servicio y los requisitos mínimos de calidad de servicio (QoS), en los que se tendrá que realizar la conexión, se produce un aumento del tamaño de los mensajes de señalización y un elevado intercambio de éstos sobre las interfaces de comunicación entre los terminales de usuario y la red, que en algunos casos (recursos radio en las comunicaciones móviles) se consumen de una forma muy poco eficiente y causan un aumento importante del tiempo de establecimiento de la sesión introduciendo retrasos indeseados que no ocurren en las redes actuales que degradan la calidad del servicio ofrecido y la experiencia del usuario.

Para resolver esta cuestión se utiliza la compresión de los mensajes de control a través del mecanismo de compresión de mensajes de señalización, SigComp, antes de de ser enviado a través de la red. Dichos mensajes son comprimidos dentro del terminal de usuario y enviados hacia la red a través de la interfaz de comunicación con la red de acceso y entregados en el punto de entrada a la red multimedia para los mensajes recibidos del usuario. En este extremo el compresor se encarga de descomprimir los mensajes que se reciben del usuario y reconstruirlo para enviarlos a la red troncal donde se transmitirán sin compresión puesto que el uso de los recursos en la red troncal es mucho menor y menos críticos que en la red de acceso. Cuando los mensajes de señalización procedentes de la red troncal hacia el usuario alcanzan el elemento de red que gestiona la comunicación con el UE, se produce nuevamente el proceso de compresión de la señalización antes de ser transmitido al terminal del usuario. A la recepción por éste de los mensajes enviados desde la red se descomprime y se recuperan los mensajes originales análogamente a como lo realiza la red multimedia con los mensajes en el sentido contrario.

4. Arquitectura de IMS

4.1. Introducción

El subsistema de red troncal multimedia IP (IMS CN) es una colección de funciones e interfaces estandarizadas que forman una red completa que se interconecta con distintas redes de acceso para proporcionar comunicaciones multiservicio a través de una única red de conmutación.

Las entidades descritas en la arquitectura de red son entidades funcionales que cubren el conjunto de acciones realizadas por la red troncal, aunque estas entidades funcionales no tienen porque corresponderse con entidades físicas, puesto que el operador decide como quiere desplegar la implementación física de tales funciones.

Dividiremos el conjunto de elementos de red según sus funciones principales:

1. Gestión de sesión y enrutamiento.
2. Bases de datos
3. Funcionalidades de Servicios y Recursos
4. Interconexión
5. funciones auxiliares y de soporte
6. Facturación

4.2. Gestión de sesión y enrutamiento

4.2.1. Introducción

Son los elementos principales de la red y realizan las acciones centrales, como la negociación, establecimiento, mantenimiento, modificación y finalización de sesiones multimedia entre usuario de la red, es decir, controlan todo el proceso de comunicación entre usuarios. Los nodos que realizan están funciones se denominan funciones de control de sesión de llamada (CSCF en inglés) y gestionan toda la señalización SIP de la sesión y dependiendo del rol que desempeñen tienen una denominación distinta. Detallamos más en profundidad cada uno.

4.2.2. Proxy Call Session Control Function (P-CSCF)

Es el primer punto de contacto dentro de la red multimedia para las comunicaciones del usuario, esto quiere decir que todo el tráfico de señalización intercambiado entre el equipo de usuario y la red se realiza a través del P-CSCF.

Esta función puede localizarse en la red local de usuario cuando éste está localizado en un área de cobertura de la red del operador (Home Network) o bien puede localizarse en una red diferente, cuando el usuario se encuentra en roaming o fuera de la cobertura de su proveedor de red (Visited Network).

Sus principales funciones son las siguientes:

- Establecimiento de conexiones de seguridad individuales con cada usuario. Negocia, establece, modifica y libera conexiones seguras y aplica los mecanismos de encriptación e integridad de la señalización intercambiada entre la red y el usuario. Actúa en cierto modo como un firewall limitando y controlando todo el tráfico que entra en la red desde un usuario y viceversa.
- Realiza funciones de filtrado al revisar la información enviada a la red por parte del terminal y la corrige o la suprime en caso de que pueda representar alguna amenaza para la misma.
- Realiza un seguimiento de los usuarios registrados a través de sí mismo y genera y almacena información de enrutamiento para sucesivas comunicaciones de cada usuario con la red.
- Compresión y descompresión de señalización desde o hacia el usuario. Debido a que el protocolo de señalización usado (SIP) contiene un elevado número de cabeceras y extensiones que pueden aumentar considerablemente el tamaño de los paquetes SIP.
- Realiza el control y la autorización de uso de los recursos de medios y la gestión de la calidad de servicio (QoS) negociada en cada sesión. Establece las conexiones necesarias con la función de aplicación de política y facturación (PCRF) y genera información de facturación relativa a cada conexión que intercambia con la red de datos de acceso utilizada para la conexión.
- Detección de sesiones o llamadas de emergencia y enrutamiento a los elementos apropiados de la red que se encargarán de su ejecución.

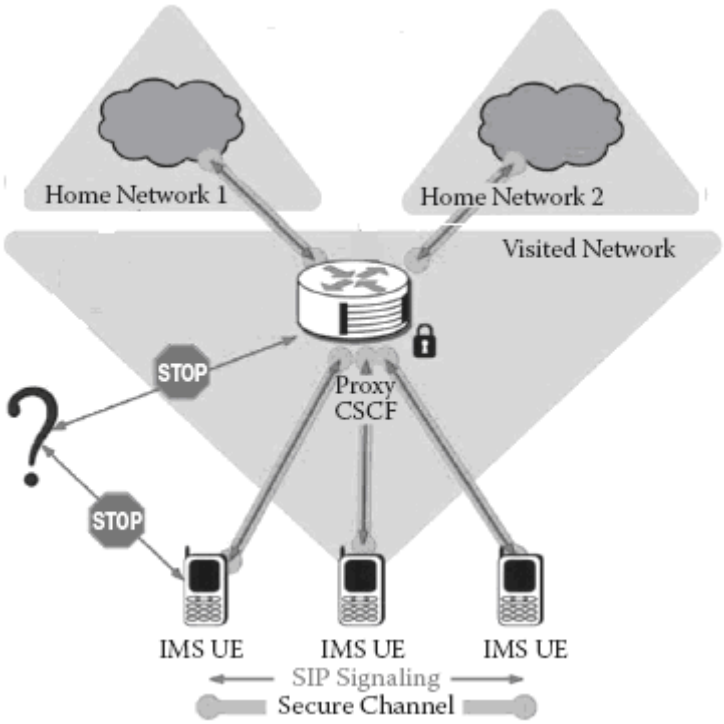

Figura 23. Esquema de conectividad de P-CSCF

4.2.3. Interrogating Call Session Control Function (I-CSCF)

Es el punto de contacto dentro de la red del operador para todas las conexiones destinadas a ese usuario. Las funciones que realiza esta entidad son:

- Obtiene la dirección del próximo elemento al que enviará la solicitud o petición a partir de la información almacenada en las bases de datos principales de la red.
- Asigna un servidor de control para un usuario con el propósito de facilitar el contacto con un elemento que realice el registro del usuario en la red.
- Realiza funciones de enrutamiento de tráfico SIP hacia servidores de control de usuario y enrutamiento de tránsito desde y hacia otras redes o dominios.
- Sólo permite la entrada de señalización proveniente de redes de confianza a través de seguridad de dominio de red (NDS).
- Puede ser utilizado como un elemento de protección de la topología de red que encripta y desencripta cabeceras con información sensible de la red en los mensajes de señalización intercambiados con otras redes.

4.2.4. Serving Call Session Control Function (S-CSCF)

Se trata de unos de los elementos principales de la red multimedia. Es la entidad encargada de crear, mantener, modificar y finalizar sesiones multimedia entre usuarios.

Las funciones centrales que realiza son:

- Realiza funciones de registro del usuario en la red, es decir valida al usuario y autoriza el acceso a los servicios ofrecidos por la red. Se apoya en los datos de los perfiles de los usuarios descargados de la base de datos principal de la red para verificar la información de autenticación proporcionada por el usuario.
- Interactúa con el nivel de aplicación, solicitando la ejecución de servicios para los usuarios.
- Determina a partir del perfil de servicio, a que servicios puede acceder y ejecutar cada usuario y se apoya en el mecanismo de criterios de filtros iniciales (iFC) para activar los servicios requeridos en función de la información recibida en las peticiones enviadas por el terminal de usuario.
- Toma decisiones de enrutamiento para transmitir una solicitud de sesión al nodo oportuno para llegar hasta el destinatario de la petición incluso si esto implica un cambio de dominio o de red.
- Proporciona suscripción a eventos del usuario y servicio. Permite recibir solicitudes de suscripción a información del estado de los usuarios y de servicios y mantiene informado al elemento que solicita la suscripción de los cambios y de los estados de los mismos.

En definitiva se encarga de todos los procesos relativos a la sesión multimedia permitiendo la comunicación con los servicios ofrecidos y con el resto de usuarios.

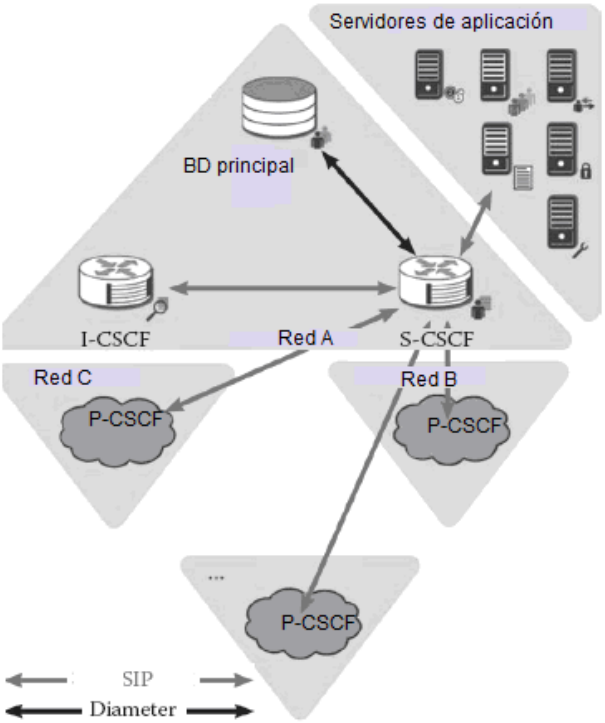

Figura 24. Comunicación entre el S-CSCF y el resto de funciones de la red troncal y de aplicación.

4.2.5. Emergency Call Session Control Function (E-CSCF)

Su función principal es gestionar las posibles solicitudes de emergencia que solicite un usuario de la red y gestiona la conexión de la llamada con un centro de emergencias. En este nodo las políticas de prioridad y disposición de recursos es diferente que para el resto de S-CSCF de la red.

Algunos de los criterios más importantes en este tipo de sesiones es la localización precisa del usuario y la clasificación del tipo de emergencia solicitada para enrutar apropiadamente estas sesiones.

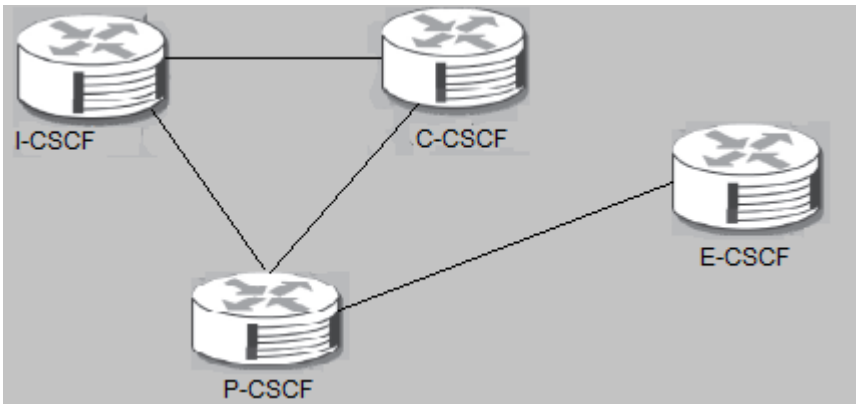

Figura 25. Esquema de relación de los diferentes tipos de CSCF.

4.3. Entidades de almacenamiento de información

Como toda red de comunicación, IMS dispone de una o varias fuentes de datos principales. Estas fuentes son las bases de datos utilizadas como soporte necesario a los elementos que gestionan las sesiones multimedia entre usuarios (CSCFs). Son dos los elementos principales, la base de datos de suscripción (HSS en sus siglas en inglés) y la función de localización de suscripción (SLF en sus siglas en inglés).

4.3.1. Home Subscriber Server (HSS)

Es la base de datos que almacena toda la información relativa a una suscripción de un usuario y que asiste a las entidades que realizan la gestión de las sesiones multimedia.

Las funciones principales que realiza son:

- Autenticación. Genera la información de seguridad de autenticación, encriptación e integridad y proporciona estos datos a la entidad encargada de gestionar las sesiones y de autenticar al usuario (S-CSCF).
- Autorización. Autoriza el acceso a la red por el usuario comprobando que no tiene ninguna restricción y autoriza el acceso a los servicios proporcionando información relevante de los mismos al usuario y a las entidades de la red troncal que lo necesiten para la invocación de éstos en el nivel de aplicación.
- Gestión de movilidad. La base de datos almacena y proporciona a las entidades de red información de la localización donde el usuario se encuentra en cada momento para entre otros determinar la entidad que controla al usuario o directamente indicando que entidad de red actualmente controla a dicho usuario.
- Gestión de las identidades del usuario. Determina y gestiona las relaciones que se establecen entre todos las identidades de un usuario, es decir, las relaciones entre las identidades públicas y privadas de cada suscriptor y en caso necesario facilita información de las mismas, por ejemplo durante el proceso de registro de un terminal de usuario en la red indicando que identidades públicas están registradas.
- Funciona como repositorio de los datos de perfil del cliente, almacenando toda clase de información relativa al usuario y proporcionando acceso a los mismos. Cuando un usuario se registra en la red, esta información es descargada directamente a la entidad que controla al usuario. La información de usuario almacenada se puede clasificar en:

    - Información de identificación, dirección y numeración. Almacenamiento de las diferentes identidades tanto públicas como privadas.
    - Información de seguridad. Información generada para la autenticación del terminal de usuario y las claves de encriptación

e integridad generadas en caso de que la autenticación sea correcta.

- Información de localización del usuario. Si el usuario ya está registrado indica que entidad de la red troncal controla a dicho usuario.
- Información del perfil del suscriptor. Toda la información relativa al usuario incluida los servicios a los que tiene acceso.

Puesto que la base de datos de suscripción gestiona, maneja e intercambia información de registro, autenticación y autorización, utiliza el protocolo de seguridad Diameter, como protocolo de comunicación a través de sus interfaces con el resto de entidades de la red troncal y del nivel de aplicación. Diameter es un protocolo definido en la RFC 3588 del IETF como el nuevo protocolo estándar de AAA evolucionado directamente del anterior protocolo que realizaba estas funciones, RADIUS, y que resuelve las limitaciones que éste presentaba.

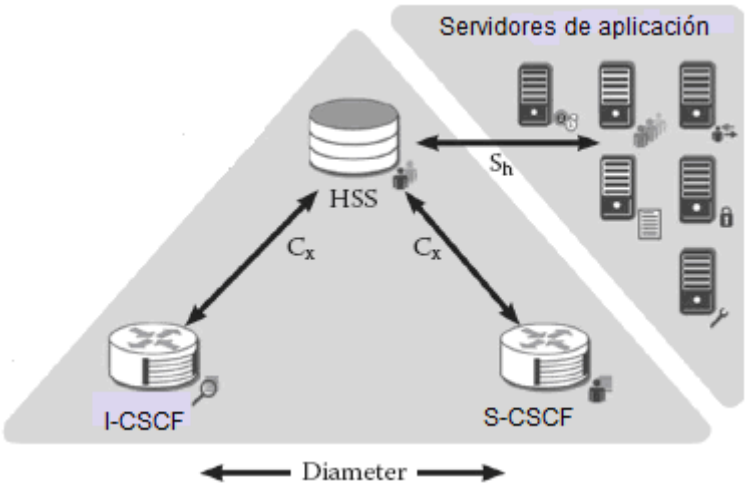

Figura 26. HSS e interfaces con otros elementos

En función de número de suscriptores, de la capacidad de la base de datos y de la arquitectura concreta de la red que tenga el operador encontraremos unos o más HSS desplegados. Cuando el operador de red despliega más de una base de datos central también se despliega el segundo elemento, la función de localización de suscripción (SLF en inglés).

4.3.2. Subscriber Location Function (SLF)

Esta entidad tiene como función, en escenarios donde se despliega más de un HSS, facilitar información a los elementos de gestión y control de las sesiones (CSCFs) de en qué base de datos se encuentran los datos de un usuario determinado para que éstos consulten a la base de datos adecuada.

La situación más habitual es cuando un I-CSCF quiere conocer en qué base de datos se encuentran almacenado los datos de una suscripción y para ello consulta a la función de localización. También es consultado durante el proceso de registro (S-CSCF) o cuando un AS requiere consultar información de un usuario para activar un servicio.

4.4. Funcionalidades de Servicios y Recursos

Las entidades relacionadas con los servicios son los servidores de aplicación (AS) y las entidades relativas a los medios y los recursos necesarios para proporcionar dichos servicios es la función de recursos multimedia (MRF en sus siglas en inglés).

4.4.1. Servidor de aplicación (AS)

Las entidades encargadas de facilitar los servicios son los servidores de aplicación (AS en sus siglas en inglés) que son los elementos que constituyen el nivel de aplicación y proporcionan servicios multimedia de valor añadido a la red. La principal función de estas entidades es albergar y ejecutar dichos servicios durante una sesión en la red. Estos servidores pueden formar parte de la propia red multimedia o estar localizado en la red de un tercero y se comunican con las funciones de gestión de sesión a través de la interfaz de control de servicios (ISC), utilizando SIP como protocolo de comunicación.

Se definen varios tipos de servidores de aplicación que pueden interconectarse con la red multimedia:

- Servidores de aplicaciones basadas en SIP.
- Servidores de aplicaciones OSA
- Servidores de aplicaciones CAMEL, o servicios personalizados para redes móviles.

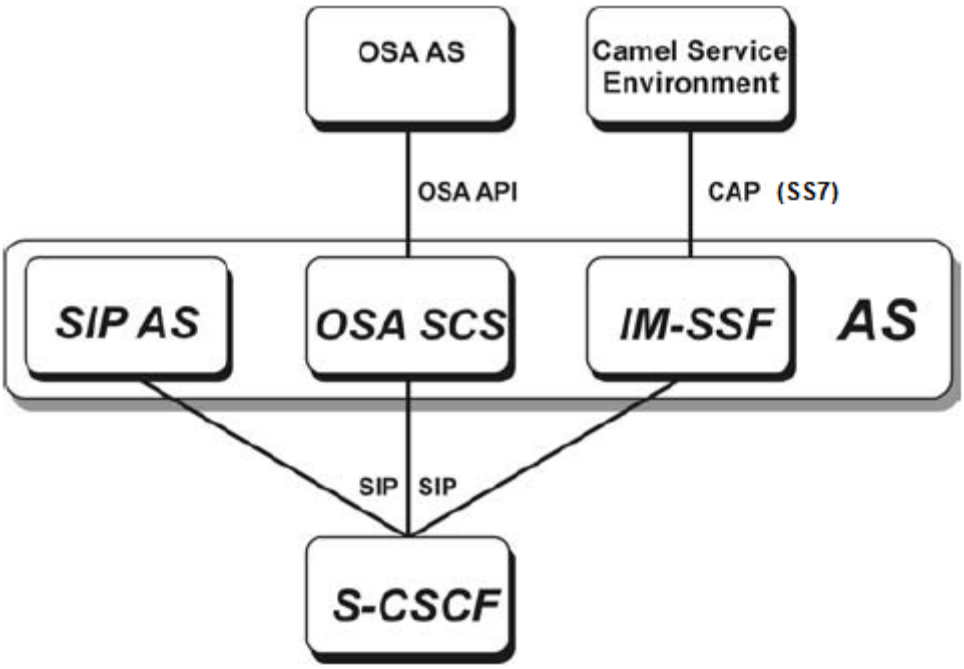

Figura 27. Traducción de protocolos de comunicación realizada por el nivel de aplicación

4.4.1.1. Servidores de aplicaciones SIP

Son el conjunto de servidores nativos de la red multimedia que ejecutan servicios multimedia desarrollados en SIP. Para proporcionar estos servicios el terminal puede actuar como un agente SIP que proporciona un servicio final, redireccionando la petición hacia un servicio externo, creando un nuevo dialogo etc.

4.4.1.2. Servidor de capacidad de servicio OSA (OSA SCS)

Facilitan una forma estandarizada y segura de acceso a los servicios desarrollados por terceros y que pueden encontrarse fuera de la propia red multimedia. Dichos servicios están creados sobre la estructura de desarrollo OSA. Esta es una estructura estandarizada, abierta y flexible que permite el desarrollo de nuevos servicios y que además incorpora un conjunto de mecanismos de seguridad (Autenticación, Autorización y registro) para el acceso seguro al servicio.

Este servidor realiza la conversión entre el protocolo de comunicación SIP de la interfaz ISC hacia el nivel de control de sesión (CSCFs) con el protocolo en la interfaz API hacia el propio servicio OSA. También hace lo mismo entre la API y la interfaz Sh con la base de datos central (HSS).

4.4.1.3. Servidor de conexión a servicios existentes (IM-SSF)

Es una servidor que se introduce para que la red soporte los servicios ya existentes, que están desarrollados a través de un entorno de servicio para aplicaciones personalizadas mejoradas (CAMEL SE en sus siglas en inglés). Este servidor interactúa con la interfaz de aplicación CAMEL (CAP en inglés). Hace por lo tanto de conversión del protocolo CAP de SS7 al protocolo SIP tanto en la interfaz ISC con el nivel de control de sesión, como con la interfaz Si, con la base de datos HSS de la red.

La siguiente figura ilustra con el nivel de control de sesión se interconecta con el nivel de aplicación y como las funcionalidades descritas interactúan con los servicios conectados a la red.

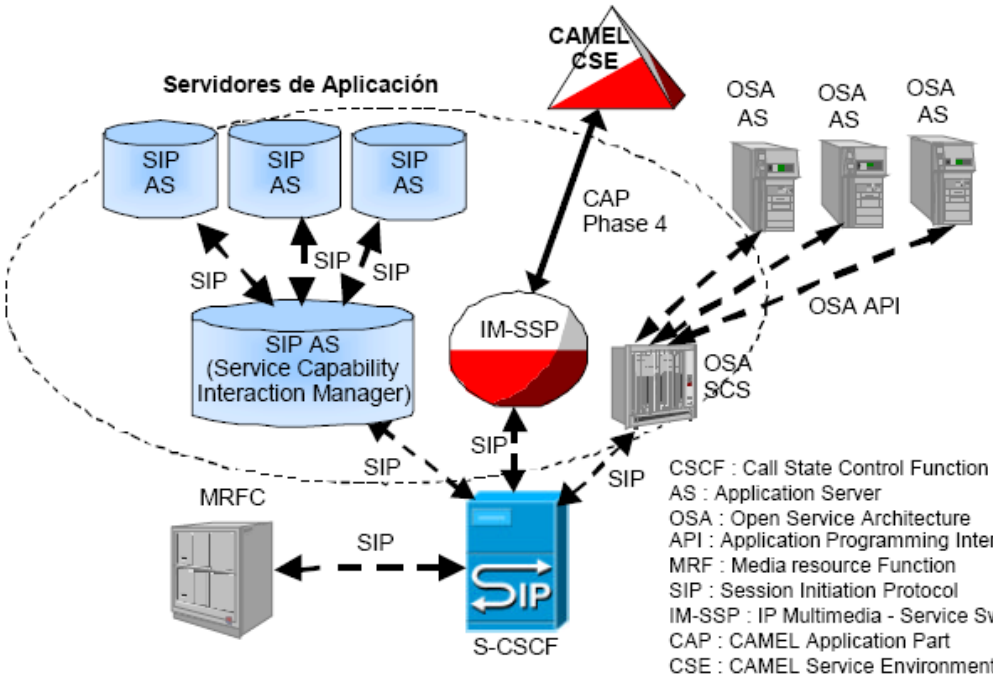

Figura 28. Arquitectura del nivel de servicios de una red multimedia.

4.4.2. Multimedia Resource Function (MRF)

La función de recursos multimedia es la función que suministra, gestiona y procesa el conjunto de recursos y medios de diversos tipos, necesarios para sustentar los servicios multimedia ofrecidos por la red.

La función de recursos se puede dividir en dos funciones:

- La función de control o gestión de los medios (MRFC en sus siglas en inglés) que es la funcionalidad que gestionará el uso de los medios.
- Y la función de procesamiento de los medios, que es la función que propiamente aporta los medios necesarios a la comunicación.

4.4.2.1. Control de recursos (MRFC)

Es la función que se comunica en el plano de señalización y recibe e interpreta la información relativa a la sesión y a los servicios que se quieren utilizar, seleccionando y controlando en base a esta información, los medios necesarios que son aportados por la función de ejecución de recursos (MRFP). La comunicación con el plano de señalización puede realizarse tanto con el nivel control de sesión (S-CSCFs) como del nivel de servicio (AS) como indica la figura.

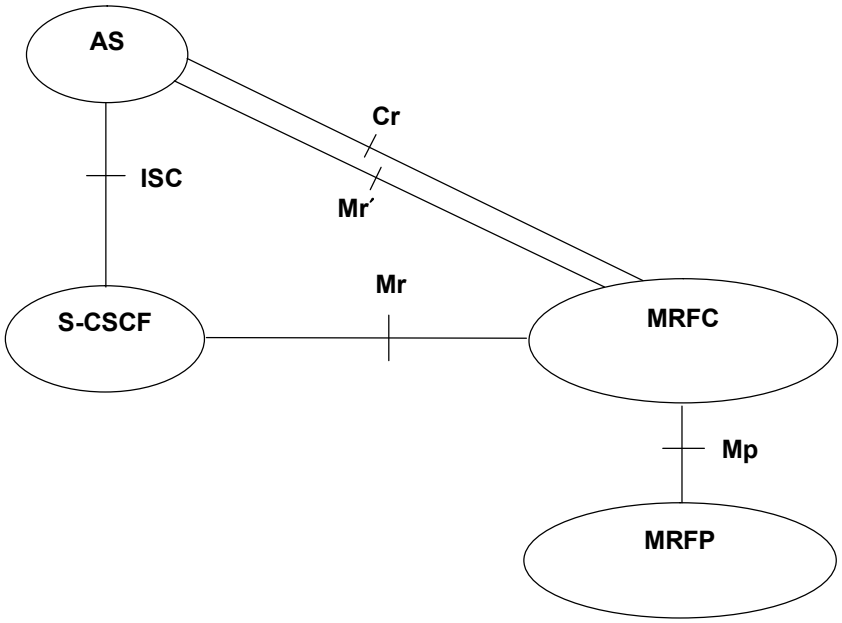

Figura 29. Arquitectura de la función de medios.

4.4.2.2. Procesador de recursos (MRFP)

Es el elemento encargado de proporcionar acceso directamente a los medios y recursos propiamente dichos y que serán controlados por el MRFC. La comunicación entre el control de medios, MRFC, y el procesador de medios, MRFP, se realiza a través de una interfaz estandarizada que usa el protocolo de comunicaciones H.248 MEGACO, usado para gestionar las funciones de medios.

Algunos de las funciones que realiza son [26]:

- Es la fuente de medios para servicios originados por la red.
- Gestión de las portadoras de medios.
- Procesado de flujos de medios, como transcodificación de medios, análisis de flujo de datos recibido etc.
- Mezcla de flujos de medios, por ejemplo cuando se reciben tráfico desde varias partes.
- Controla como se produce el acceso a los medios y que éste se haga de la forma adecuada.
- Generación de registros de datos de llamada o sesión para las funciones de facturación.

4.4.2.3. Gestor de recursos multimedia (MRB)

Entidad funcional que se encarga de recopilar y suministrar información de las diferentes funciones de recursos multimedia MRF desplegadas en la red a las entidades de control que usan estos recursos.

El MRB a partir de las necesidades de recursos de las diferentes aplicaciones o servicios solicitados se encarga de determinar qué función de recursos multimedia MRF de las desplegadas en la red satisface mejor dichas necesidades. Entonces selecciona y asigna información de esa función de recursos al servicio o aplicación en cuestión [26].

La información que tiene en cuenta cuando asigna una función de recursos MRF a una aplicación es:

- Los requisitos específicos que tienen que tener los medios para la aplicación o servicio requerido.
- La identidad de la aplicación o servicio.
- Criterios de calidad de servicio (QoS) o de nivel de servicio (SLA).
- Recursos que ya pudiera tener asignados la aplicación.

Para realizar correctamente la asignación de recursos, el MRB necesita conocer la siguiente información también:

- Disponibilidad de las funciones de recursos y los atributos de cada una.
- Información de que funciones están asignadas a ciertos recursos.
- Información de capacidad máxima de las funciones de recursos.

La función MRB puede desplegarse en la red de dos formas distintas.

4.4.2.3.1. Modo consulta

La aplicación hace una consulta por medio de la interfaz Rc al MRB, que asigna una función de recursos a la aplicación y le indica la dirección del MRF asignado. La aplicación envía una petición directamente al MRFC o a través del S-CSCF usando la dirección proporcionada por el MRB. Cuando el AS está utilizando los recursos notifica esto al MRB para que este registre la asociación [27].

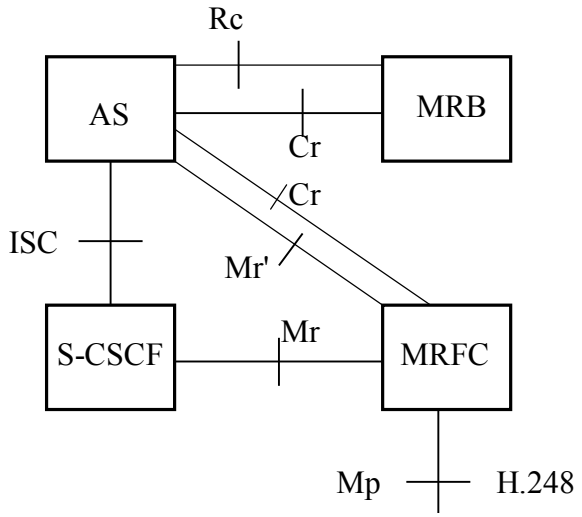

Figura 30. La aplicación solicita directamente los recursos a la MRF asignada por el MRB

4.4.2.3.2. Modo en línea

En este caso el MRB se encuentra entre la aplicación (AS) y la función de recursos (MRFC y MRFP). La aplicación envía una petición de recursos indicando los atributos que estos tiene que tener y el MRB determina que MRF se ajusta más a esa petición y envía la petición directamente, o a través del S-CSCF, al MRFC en cuestión, es decir la comunicación entre la función de recursos, MRFC y la aplicación se realiza a través del MRB [27].

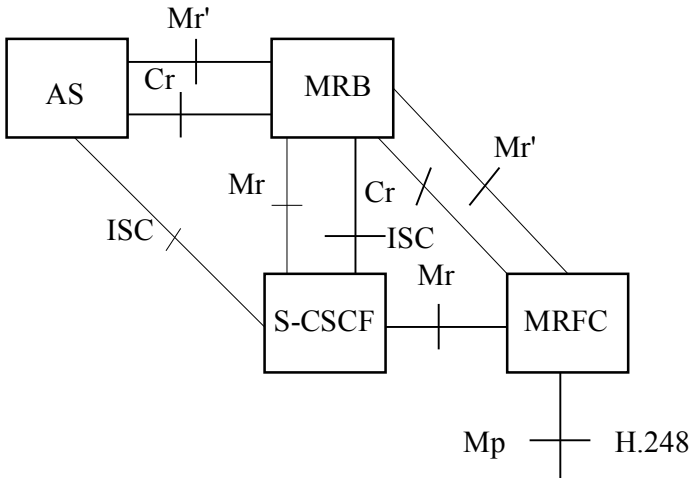

Figura 31. Comunicación entre la aplicación y la función de recursos a través del MRB.

4.5. Interconexión e interoperabilidad

Una de las capacidades más importantes de la red multimedia es la posibilidad de interconectarse con distintas redes de datos y circuitos existentes para que los usuarios de la red multimedia puedan comunicarse con usuarios de otras redes, facilitando la interoperabilidad con múltiples usuarios, independientemente del tipo de red y de la clase de terminal que utilizan.

Para que esta funcionalidad pueda ser implementada, es necesario desarrollar un conjunto de entidades o funciones de interconexión que son:

- Función de control de la pasarela de medios (MGCF).
- Pasarela de señalización (SGW).
- Pasarela de medios de la red multimedia (IMGW).
- Función de control de interconexión (IBCF).
- Pasarela de transición (TrGW).

De las funciones mencionadas anteriormente algunas de ellas se emplean para interconectar con redes conmutadas de circuitos y otras se emplean para la conexión con otras redes conmutadas de paquetes.

4.5.1. Interconexión con redes conmutadas de circuitos

En el caso de interconectarse con redes heredadas de conmutación de circuitos como la red telefónica básica (PSTN en su acrónimo en inglés) la red digital de servicios integrados (ISDN) o el dominio de conmutación de circuitos de las redes móviles terrestres (CS PLMNs) se desarrollan un conjunto de funciones que permiten comunicar un usuario de la red multimedia y un usuario que pertenezca a una de estas redes existentes. Estas funciones tienen como fin llevar a cabo las conversiones y transcodificación necesarias para adaptar la información de los protocolos y los medios utilizados en el plano de señalización y en el plano de usuario de cada red a los empleados en la otra red para asegurar la completa interoperabilidad entre dominios [26].

4.5.1.1. Función de control de la pasarela de medios (MGCF)

Se trata de un componente central de la red troncal multimedia que tiene como tareas principales:

1. Convertir los mensajes de señalización SIP, recibidos del control de la sesión (CSCFs), a través del BGCF o de éstos directamente, a los protocolos de señalización de las redes conmutadas de circuitos, ISUP/BICC (que forman parte del nivel aplicación del sistema de señalización SS7) [28]. También adapta los protocolos de transporte TCP/UDP al protocolo de transporte de SIGTRAN, SCTP, en caso de

que el transporte no se estuviera ya realizando sobre este último protocolo.

2. Controla la pasarela de medios (IMGW) a través del protocolo de comunicación H.248 MEGACO.

3. Se comunica con la pasarela de señalización (SGW) a la que envía la señalización del nivel de aplicación convertida, de SIP a ISUP/BICC.

4. Además determina cual es el siguiente paso en el enrutamiento de llamadas entrantes provenientes del dominio de circuitos.

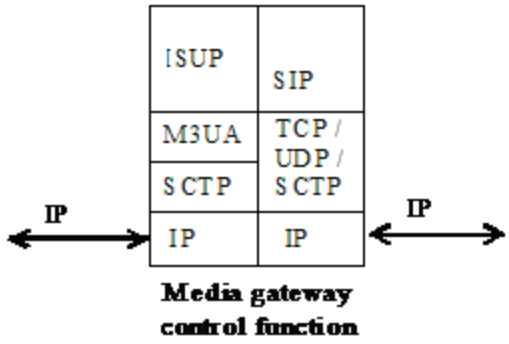

Figura 32. Conversión de protocolos de aplicación

4.5.1.2. Pasarela de señalización (SGW)

Se encarga de realizar el mapeo de los protocolos de transporte de señalización de SIGTRAN, M3UA-SCTP/IP a MTP sin entrar en el nivel de aplicación (la conversión de SIP a ISUP/BICC la realizó MGCF). Esta funcionalidad se comunica hacia la red multimedia con el MGCF y por el otro lado se comunica con el punto de señalización SS7 en la red conmutada de circuitos [28].

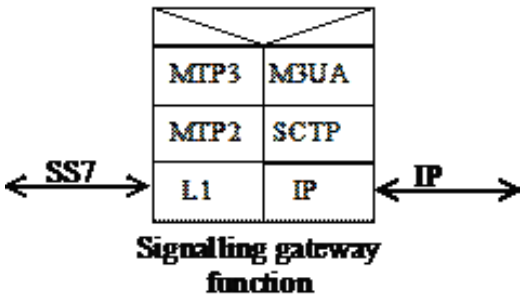

Figura 33. Conversión de los protocolos de transporte de la señalización entre redes

4.5.1.3. Pasarela de medios de la red multimedia (IMGW)

La pasarela de medios es el elemento encargado de convertir los protocolos y los formatos utilizados en los medios de cada red interconectada. Mapea el protocolo RTP de transporte en tramas del tráfico de usuario en la red de paquetes, al protocolo utilizado en los dominios de circuitos conmutados, mayoritariamente, canales de portadoras TDM (PCM de 64Kbps)[28].

A su vez, mapea formatos entre dominios disponiendo de sus propios recursos para realizar procesamiento de señales, transcodificación y adecuar la información al medio correspondientes (aplicación de canceladores de eco, etc.).

A continuación incluimos un ejemplo de cómo sería la conversión tanto en protocolos como en formatos realizada por la pasarela multimedia, donde se ilustra como esta funcionalidad adapta el formato del tráfico de usuario (códec AMR a PCM G.711) y las tramas en las que se encapsulan dichos formatos (tramas RTP/IP a canales de portadora TDM).

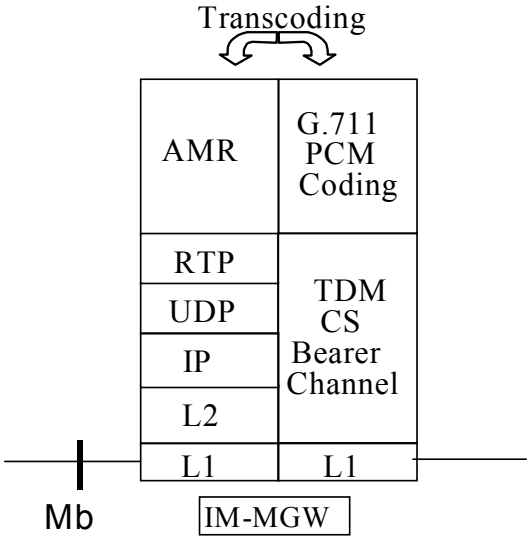

Figura 34. Conversión de protocolo y formatos en el plano de usuario

El esquema completo de interconexión entre la red multimedia y el dominio de circuitos conmutados es el que se muestra abajo, donde se puede observar la relación establecida entre las diferentes entidades funcionales y la conversión de protocolos que realiza cada entidad.

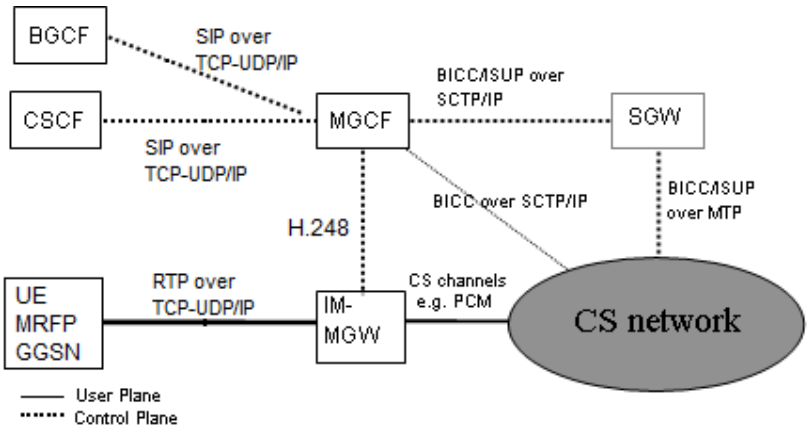

Figura 35. Diagrama completo de interconexión de la red multimedia con la red conmutada de circuitos

4.5.2. Interconexión con redes conmutadas de paquetes

La red multimedia también se interconecta con diferentes redes de datos como otras redes multimedia, Internet (redes WAN y LAN), dominio de paquetes de redes móviles terrestres (GRPS, HSDPA, etc.), redes fijas de cable o fibra, redes privadas corporativas (IPBX) y en general cualquier red de conmutación de paquetes sobre IP [26]. Para permitir la comunicación entre usuarios de diferentes dominios IP, se despliega un conjunto de funcionalidades que permitirán la comunicación sobre este conjunto de protocolos comunes, facilitando la conversión de protocolos y formatos.

4.5.2.1. Función de control de interconexión (IBCF)

Es el elemento encargado de controlar la interconexión entre el extremo de la red multimedia IP y otras redes actuando por lo tanto como punto de entrada a la red y como punto de salida para las redes IP. Sus principales tareas son la monitorización y ajuste de la señalización SIP, la aplicación de política de protección y privacidad a la topología de red, el control sobre la transcodificación de medios (versiones del protocolo IP y conversión de formatos o codificaciones de los datos en caso de incompatibilidad entre los ofrecidos por una de las redes en la oferta SDP y los soportados por la otra).

Para estas funciones se apoya varias entidades internas o externas:

- Pasarela de nivel de aplicación (IMS-ALG)
- Pasarela de transición o transporte (TrGW)
- Pasarela de encriptación de la topología de red (THIG)

4.5.2.1.1. Pasarela de nivel de aplicación (IMS-ALG)

Funcionalidad interna del IBCF que adapta la información y los campos de cabeceras y cuerpo de mensaje de los protocolos del nivel de aplicación, SIP/SDP, para que esta información se ajuste a la estructura de las versiones IPv6 o IPv4 indistintamente, es decir, si dos dominios que utilizan como protocolo de transporte IP con diferentes versiones se quieren comunicar, esta función se encarga de mantener diálogos separados con cada dominio y adaptar la información SIP/SDP contenida en los mensajes para que sea entendida por cada dominio.

4.5.2.1.2. Pasarela de Transporte (TrGW)

Funcionalidad que realiza la traducción de direcciones, puertos y protocolos (NAPT-PT) estableciendo asignaciones dinámicas entre direcciones y puertos de un rango de IPv4 a direcciones y puertos de un rango de IPv6 y viceversa, adaptando todos los campos necesarios en las

cabeceras de la trama IP permitiendo la conversión completa del protocolo de transporte.

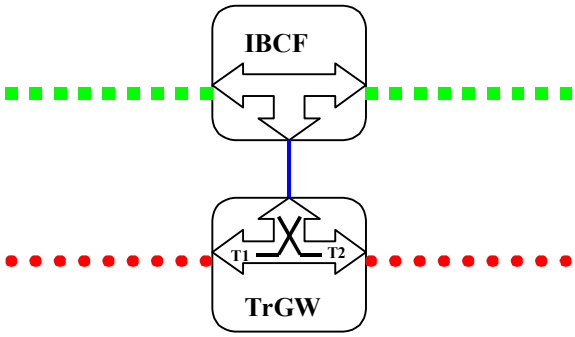

Figura 36. Control de la pasarela de interconexión por la función de interconexión.

4.5.2.1.3. Pasarela de encriptación de la topología de red (THIG)

Es la funcionalidad encargada de controlar que los datos sensibles de la red multimedia, como es el caso de la topología interna de la red multimedia, no sean publicados hacia dominios externos. Esta función aplica políticas de privacidad modificando todas las cabeceras necesarias que revelen información de topología de la red en mensajes de señalización que se intercambien con otros dominios o redes.

4.6. Función de control de política de la red y de tarificación (PCC)

Es la entidad funcional encargada de determinar como la política definida por el operador de red debe ser aplicada en cada situación y de generar los cargos oportunos en función de los flujos de datos de servicios utilizados por cada usuario, es decir, es la función encargada de comunicar los niveles de control y señalización, con el nivel de transporte y hacer cumplir las condiciones acordadas en la señalización de las sesiones en las redes de acceso de cada usuario.

Esta entidad funcional está compuesta a su vez de dos elementos que realizan las funciones anteriores. Un elemento encargado de la toma de decisiones de política a aplicar en cada momento, denominado función de reglas de política y tarificación (PCRF en su acrónimo en inglés) y un elemento encargado de ejecutar las decisiones tomadas por el elemento anterior denominado función de ejecución de política y tarificación (PCEF en su acrónimo en inglés).

El control de política y facturación se encarga de llevar a cabo los siguientes procedimientos [26]:

- Autoriza los recursos de QoS a emplear.

  El PCRF calcula y emite cual debe ser la autorización de recursos para cada sesión en la red multimedia expresados en términos de recursos IP.

La autorización se basa en la información derivada de los mensajes SDP intercambiados durante la negociación de la sesión que es facilitada al PCRF por el P-CSCF.

- Realiza la reserva de recursos en las redes de acceso.

  El PCEF se encarga de ejecutar la reserva de recursos IP en la red de acceso estableciendo una portadora de servicio que se ajuste a la autorización de recursos emitida por el PCRF. El proceso se realiza a través del mapeo de la información de la autorización de recursos emitida en atributos propios de calidad de servicio en la red de acceso.

- Habilita y deshabilita el paso de flujos de medios.

  El PCRF se encarga de la activación y el bloqueo del uso de los recursos IP reservados por el PCEF para los flujos de medios autorizados de cada sesión multimedia. El PCEF restringirá el acceso del equipamiento del usuario a los recursos reservados hasta que reciba la indicación de acceso por parte del PCRF manteniendo cerrado el paso hasta ese momento

- Revoca la autorización previa de recursos.

  El PCRF emite una orden de desactivación de los recursos IP previamente autorizados y asignados a un usuario para una sesión multimedia en curso. El PCEF ejecuta la desactivación de recursos dentro de la red de acceso.

- Autoriza la modificación de recursos empleados en la red de acceso.

  Se produce cuando un equipo de usuario solicita la modificación de los parámetros de la portadora IP de la red de acceso solicitando unos nuevos requisitos de QoS para la misma. En este caso el PCEF inspecciona si tiene permiso para modificar los recursos reservados actualmente en el caso de que los nuevos parámetros requeridos estén dentro de los recursos autorizados previamente o si por el contrario necesita emitir una solicitud de modificación de recursos reservados al PCRF. Este elemento a su vez en base a la información de la petición de recursos y de la sesión actual emite una autorización de modificación para el PCEF. Cuando éste recibe la autorización inicia la reserva de una nueva portadora IP que se ajuste a la nueva autorización de recursos asignados y procede a la liberación de la antigua portadora.

- libera recursos desde la red de acceso.

  Cuando un usuario desea liberar los recursos asociados a una conexión previa, el PCEF emite una petición de liberación de recursos hacia el PCRF que puede ser utilizada para ser reenviada a través del P-CSCF para liberar los recursos correspondientes a la red de acceso del usuario remoto.

4.6.1. Función de decisión de política de red y de facturación (PCRF)

Es la entidad funcional encargada de determinar cuáles serán las decisiones y las reglas de política de red a aplicar en cada momento en la red multimedia y en las redes de acceso. Para determinar las decisiones se apoya en la información relativa a la sesión y a los medios solicitados, que le proporciona el punto de contacto del nivel de control con el terminal de usuario, el P-CSCF. Esta información es derivada principalmente de los mensajes de señalización SIP/SDP respecto a los medios solicitados por el usuario para cada servicio y a la información recibida del repositorio de perfiles del suscriptores para determinar, si el usuario puede acceder a los recursos y servicios solicitados y habilitar el mapeo de la información de los medios solicitados por el usuario a los recursos necesarios de QoS que tienen que ser satisfechos (identificador de clase de QoS autorizada, tasas de transferencia permitidas, etc.) para soportar dichos flujos de medios en el caso de que el usuario obtenga acceso a los servicios del sistema. A su vez esta entidad controla el acceso y el uso que haga el usuario durante toda la sesión de los recursos proporcionados por la red para en caso de requerirse una modificación o restricción, pueda actuar sobre los mismos y pueda comunicar al nivel de control, P-CSCF, como proceder en cada momento [30].

Este control del uso de los recursos también tiene como objetivo cuantificar el uso de los recursos por parte del usuario para genera información de facturación relativa al mismo e intercambiar esta información con la red de acceso de conectividad IP (IP-CAN) que generará su propia información de facturación, con el propósito de correlar ambos datos y verificar que la información de tarificación es correcta y aplicable.

Este elemento se comunica directamente y controla la función de ejecución de política y facturación (PCEF) que será la que aplicará las decisiones tomadas por esta entidad asegurándose que los flujos de datos se ajustan a las políticas definidas por el operador, a la información del perfil de suscriptor y a recursos autorizados por parte del PCRF. La función de control de política y facturación se comunica con el punto de control del usuario, P-CSCF, a través del protocolo de comunicación DIAMETER.

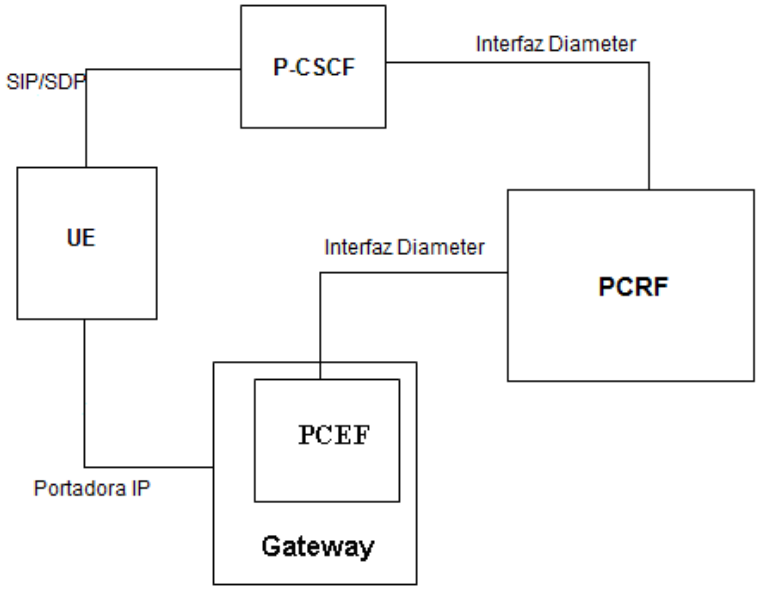

Figura 37. Comunicación de la función de política con el nivel de control y con el nivel de usuario.

4.6.2. Función de ejecución de política y tarificación (PCEF)

Esta funcionalidad está localizada en la pasarela que conecta con el terminal de usuario, el GGSN de la red GPRS o el PGW de la red EPS, y se encarga de interpretar y ejecutar todas las órdenes recibidas de la función de decisión de política (PCRF) permitiendo o no que el usuario disponga y haga uso en caso afirmativo de los recursos necesarios para los servicios autorizados.

Proporciona entre otras, detección y medición de flujos de datos de servicios y su correspondiente generación de información de facturación, gestión y control del tráfico de usuario, ejecución y mapeo de parámetros de calidad de servicio autorizados y en algunos casos se encarga también de proporcionar gestión de la señalización de la sesión.

La función de ejecución de política lleva a cabo las decisiones tomadas en el PCRF centrándose en varios aspectos [30]:

1. Control acceso. Permite sólo el paso de los flujos de datos de servicios que tengan la correspondiente autorización por parte del control de política (PCRF).

2. Ejecución de nivel de servicio. De acuerdo a la regla de política activa en cada momento, proporciona la calidad de servicio autorizada para cada flujo de datos del servicio.

3. Mapea los parámetros de QoS que han sido autorizados por el nivel superior a los parámetros específicos de calidad en la red de acceso de conectividad IP (IP-CAN) y se asegura que los recursos utilizados están dentro del grupo de recursos permitidos para cada flujo de datos de servicio.

La función de ejecución de tarificación permite solo el paso a los flujos de datos de servicios que cumplen las condiciones marcadas por los sistemas de tarificación de la red.

4.7. Funciones auxiliares

En este apartado describimos algunas entidades funcionales que realizan funciones importantes de soporte y que asisten a la red para completar algunas de las funciones anteriormente mencionadas. Estas son:

- Función de salida de la red multimedia (BGCF)
- Pasarela de seguridad (SEG)
- Función de recuperación de localización (LRF)

4.7.1. Función de salida de la red multimedia (BGCF)

Es la función encargada de determinar donde se realiza la salida de la red multimedia para una sesión. Cuando las funciones centrales de la red troncal determinan que la sesión no puede ser enrutada con los mecanismos habituales (DNS, ENUM) entonces dentro de la red multimedia se reenvían los mensajes de señalización hacia esta función que determinará cuál es el próximo paso en el enrutamiento de la señalización SIP a partir de diferentes fuentes de información disponibles (bases de datos, información administrativa, información recibida por otros medios etc.) [31].

Se pueden dar diferentes casos:

1. La función determina que la red en la que se terminará la sesión, es una red conmutada de circuitos, y que la salida hacia dicha red se produce desde la propia red donde se encuentra la función de salida (BGCF), entonces esta función se encarga de entregar los mensajes de la sesión a la función de control de la pasarela multimedia (MGCF) que realizará directamente la interconexión con el dominio de circuitos [26].

2. Si la función de salida (BGCF) determina que la red conmutada de circuitos en la que se terminará la sesión no está interconectada con la propia red multimedia, entonces enviará a la función de salida (BGCF) de una red de transito los mensajes de la sesión para que esta entregue los mismos a la red de circuitos de destino a través del MGCF correspondiente [26].

3. Si la función de salida determina que la sesión se terminará en otra red multimedia u otra red IP, entonces la señalización se entregará al punto de entrada y salida hacia otras redes IP en la propia red multimedia, la IBCF, que se encargará de enviar los mensajes de la sesión hacia la red deseada [26].

Dentro de una misma red de un operador pueden existir múltiples BGCF.

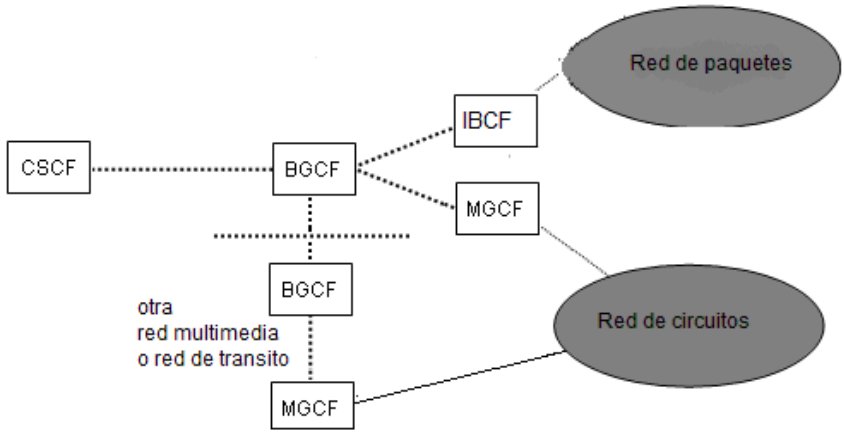

Figura 38. Esquema de interconexión de un BGCF

4.7.2. Pasarela de Seguridad (SEG)

Como se explico en el apartado de seguridad 3.2.4, las pasarelas de seguridad son las entidades emplazadas en los extremos de cada dominio de seguridad que se comunican con otras pasarelas de seguridad en los bordes de otros dominios o redes de seguridad y que tiene por función principal ejecutar la política de seguridad determinada por el operador para todo el tráfico de entrada y de salida del dominio de seguridad forzando a que todo el tráfico IP de señalización entre dominios pase a través de estas funciones para su control y tratamiento[22].

4.7.3. Función de recuperación de localización (LRF)

Es una funcionalidad auxiliar que proporciona información precisa de localización de un usuario en la red multimedia como soporte a servicios de emergencia. Proporciona posición inicial del usuario, información actual y actualización de la posición. En base a esta información la función de decisión de enrutamiento de emergencia determinará hacia qué centro de emergencias la llama tiene que ser enviada [32].

4.8. Funciones de tarificación

4.8.1. Introducción

Las funciones de tarificación, son aquellas que permiten recolectar la información generada por las entidades de la red, relativa al uso de los recursos y los servicios por parte de los usuarios, y enviarla al sistema de facturación para su aplicación en el saldo o balance del cliente. Los modelos de tarificación empleados en la red multimedia se basan en los principios de tarificación por sesión o tarificación por servicio o evento que permite la tarificación de una forma flexible y ajustada a los recursos utilizados por cada cliente.

Para la aplicación de estos principios la red multimedia tiene que realizar control y monitorización en tiempo real del uso realizado de los recursos disponibles en la red (control de recursos realizado por PCRF/PCEF) para detectar los eventos que deben ser cargados.

Toda la información enviada desde la red hacia las funciones de tarificación se compila en un registro de sesión, llamada o evento llamados CDR (en sus siglas en inglés) que contiene toda la información relevante de una sesión o del uso de un servicio (como información del suscriptor, recursos y servicios utilizados, información estadística de la sesión o evento etc.) para permitir la rápida determinación de los cargos a realizar al cliente por parte del sistema de facturación. Esta información generada tiene además una finalidad estadística y de soporte muy importante puesto que asiste a las estructuras de operación y mantenimiento de la red (O&M) y de gestión administrativa y atención al cliente.

4.8.2. Arquitectura de los sistemas de tarificación

Debido a la diferente forma de aplicar estas funciones se establecen dos modelos o arquitecturas de tarificación diferenciados:

- Sistema de tarificación online o en tiempo real, donde el usuario sólo puede hacer uso de los servicios si previamente el sistema de tarificación permite el acceso a los mismos, lo que ocurre cuando el usuario dispone de una cantidad suficiente de saldo en su cuenta. Los cargos por servicios usados se realizan en el momento y el control del balance del cliente se hace en tiempo real.

- Sistema de tarificación offline o post-pago, donde el usuario no tiene restricciones en tiempo real de acceso a los servicios por cuestiones de saldo y donde después de cada servicio utilizado se transfiere información al sistema de facturación, para que pasado un periodo de tiempo, el operador emita una factura sobre la cuenta del cliente, con todos los servicios utilizados por ese cliente en el periodo de tiempo dado.

Para satisfacer estos dos casos, se despliegan en la red multimedia las arquitecturas que satisfacen estos modelos y que son, el sistema de tarificación online (OCS) y las funciones de tarificación offline (OFCS)

4.8.3. Funciones de tarificación offline o diferido (OFCS)

Son el conjunto de funciones o entidades que recopilan información de tarificación relativa al uso de los recursos de la red, generada por las entidades troncales de la red de forma simultánea al uso de cada servicio, pero que no requiere que los usuarios tengan autorización previa al acceso a los recursos. Este mecanismo no interrumpe o restringe al acceso a los servicios prestados al usuario en tiempo real si no que difiere el control de la facturación a un momento posterior. Estas entidades generan registros de información de sesión (CDRs) que son enviados a los sistemas de facturación del operador para después de un periodo de tiempo determinado, emitir el correspondiente adeudo en la cuenta del cliente [33].

En el sistema de tarificación diferido prácticamente todas las entidades de la red troncal multimedia facilitan información hacia el sistema de tarificación diferida (OFCS) como se indica en la ilustración 26. También algunas entidades en las redes de acceso (PCEF en la pasarela de red de acceso de datos (GGSN o P-GW)) envían información hacia el sistema de tarificación.

Este mecanismo de tarificación está compuesto por las siguientes funciones:

- Función de activación de tarificación (CTF)
- Función de información de tarificación (CDF)
- y Función de pasarela de tarificación (CGF)

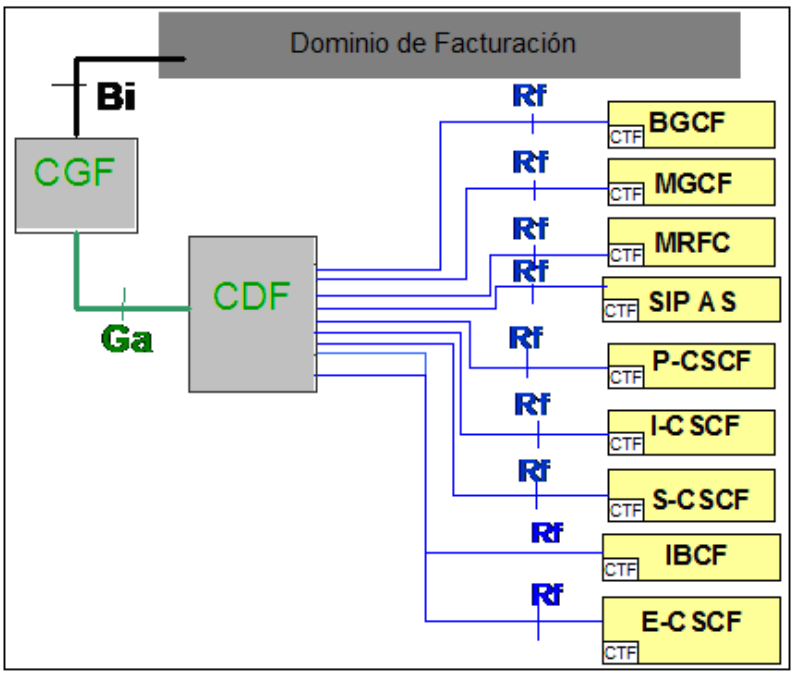

Figura 39. Arquitectura de sistema de facturación offline en la red multimedia

4.8.3.1. Función de activación de tarificación (CTF)

Es la función encargada de generar eventos o sucesos de tarificación en base al uso de los recursos del sistema por parte de los usuarios. Se encarga de recoger toda la información relativa al uso de los recursos, asocia ésta a los eventos tarificables que crea esta función y lo envía a la función de datos de tarificación (CDF) para su procesado. Este componente está presente en todas las entidades de red que monitorizan el uso de los recursos del sistema y que proporcionan información del mismo a las funciones de tarificación y facturación por lo que su despliegue dentro de las entidades de red es obligatorio [33].

Las funciones indicadas se satisfacen con dos bloques funcionales:

- Recopilación de información de registro

  Establece que flujos de datos de señalización, tráfico de usuario o servicios se monitorizarán, las condiciones que se tienen que cumplir para que se active la recopilación de información, y una vez que se activa la función que información se recogerá y las relaciones entre servicios, portadoras, sesiones y usuarios correspondientes.

- Envío de información de registro

  Detecta que eventos tarificables se ajustan a la información reunida y reenvía dichos eventos, que contienen toda la información relevante junto con un identificador de los usuarios

relacionados, a la función de datos de tarificación CDF, a través de la interfaz Rf, usando el protocolo de seguridad Diameter.

4.8.3.2. Función de datos de tarificación (CDF)

Es la función que recibe los eventos tarificables enviados por el CTF y utiliza esta información para construir los registros de sesiones o llamadas (CDRs) con un contenido y un formato concreto y definido. El procedimiento para la generación de registros sigue algunas reglas [33]:

- Cada evento tarificable solo puede ser parte de un único registro (CDR).
- Un registro puede estar formado por uno o más eventos tarificables.
- No es obligatorio que exista sincronización entre la recepción de un evento tarificable y la composición del registro posterior, es decir, no es necesario que se realice en tiempo real.
- Todos los eventos que forman parte de un mismo registro deben provenir del mismo elemento de red.

4.8.3.3. Función de pasarela de tarificación (CGF)

Esta función es la responsable de recibir los registros de sesión o llamada (CDRs) generados por la función anterior a través de la interfaz Ra, empleando también el protocolo de seguridad Diameter, y retransmitirlos al sistema de facturación del operador, es decir, actúa como pasarela de interconexión entre la función de generación de registros y el dominio de facturación.

Las tareas principales de esta función son:

- Recepción de CDRs, puede recibir registros de múltiples CDFs desplegados.
- Pre-procesamiento de CDRs como validación, reformateo o almacenamiento, gestión de errores y otros.
- Enrutamiento, filtrado y gestión de CDRs para una gestión optimizada.
- Transferencia de los registros hacia las bases de datos.

4.8.4. Sistema de tarificación online o en tiempo real (OCS)

Es el conjunto de funciones que proporcionan a los usuarios autorización de acceso a los recursos de la red, previa al uso de los mismos. Cuando la red recibe una petición de acceso a los recursos, obtiene la información de tarificación relevante y

envía la información en tiempo real al sistema de tarificación online que generará una autorización de acceso a los recursos limitada, que obligará a que cada determinado tiempo tenga que ser renovada mientras el usuario hace uso de los recursos del sistema [33].

A diferencia del sistema de facturación diferido, no todas las entidades de la red troncal se comunican con las entidades del sistema de tarificación. En la siguiente ilustración se muestra como sólo la función de control de recursos multimedia (MRFC), los servidores de aplicación (SIP-AS) y el elemento de control de sesión (S-CSCF) se interconectan con el sistema de tarificación online (OCS). También se interconectará con entidades de las redes de acceso (GGSN -P-GW/PCEF).

La generación de registros (CDRs) no es absolutamente necesaria para el funcionamiento de sistema de tarificación online puesto que este tiene que autorizar el acceso a los recursos previamente a su uso, sin embargo como hemos comentado estos registros son importantes para las tareas de administración y operación del operador. Para que el sistema online pueda generarlos, conecta con las funciones CDF y CGF explicadas en el sistema de pospago para su generación y su envío a las bases de datos correspondientes como se muestran en la ilustración 27.

Las funciones que componen este sistema son:

- Función de activación de tarificación (CTF)
- Funciones de facturación online (OCF)
- Función de gestión de saldo/balance de la cuenta (ABMF)
- Función de tarificación o valoración (RF)

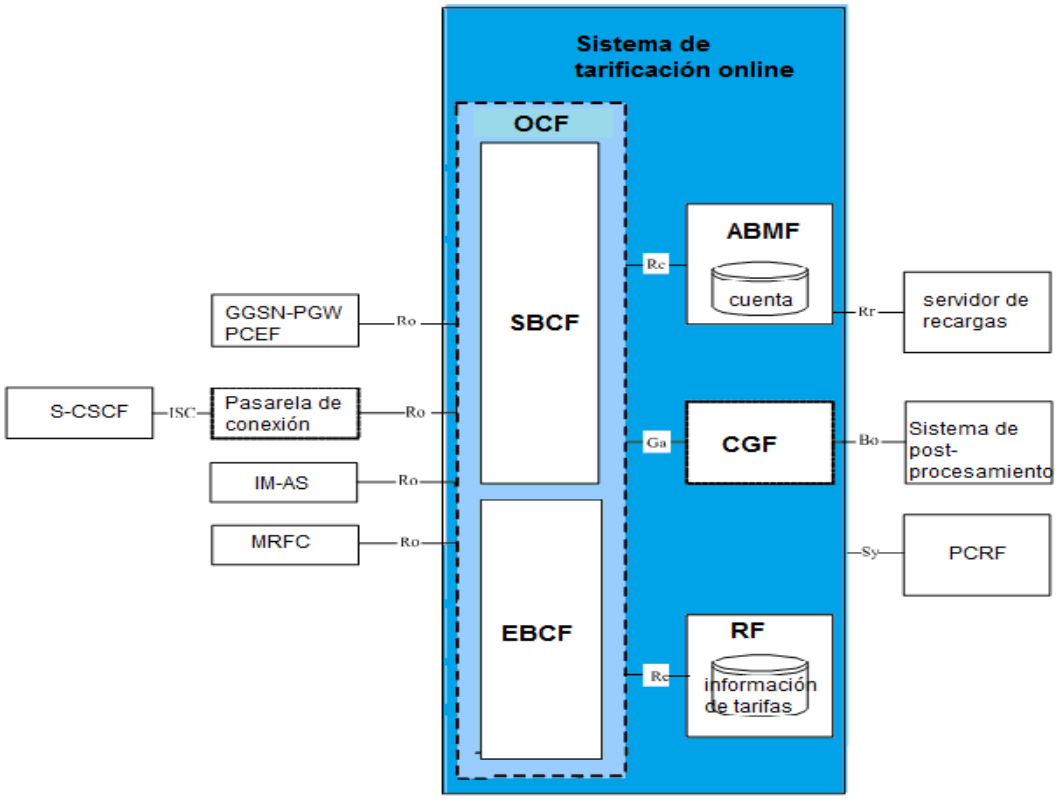

Figura 40. Arquitectura funcional del sistema de tarificación en tiempo real

4.8.4.1. Función de activación de tarificación (CTF)

En esencia es la misma función que para el sistema de tarificación diferido. Recopila información relevante del uso de los recursos del sistema, genera eventos tarificables y los transmite a la función de tarificación online (OCF) pero con algunas modificaciones en el bloque funcional de retransmisión de información con respecto al anterior sistema [33].

- Los eventos son enviados para obtener autorización para el uso de recursos solicitados por el usuario.
- Debe ser capaz de retrasar el acceso y el uso de los recursos hasta que la función OCF haya confirmado el acceso a los mismos.
- Debe realizar un seguimiento del estado de la autorización de acceso a los recursos durante el uso de los mismos.
- Debe ser capaz de ejecutar acciones para terminar o restringir el acceso a los recursos una vez que la autorización haya expirado o no haya sido confirmada.

El envío de la información y los eventos se realiza a través de la interfaz de comunicación Ro en tiempo real, que utiliza el protocolo de seguridad Diameter para la comunicación entre el CTF y OCF. La interfaz soportar la comunicación en modo de sesión (tarificación basada en sesiones) y en modo aislado (tarificación basada en eventos concretos).

4.8.4.2. Función de tarificación en tiempo real (OCF)

4.8.4.2.1. Tarificación por evento (EBCF)

Realiza la tarificación y el control de crédito por evento en el nivel de portadora, de sistema y de servicio, es decir, en base al contenido de las portadoras, de los recursos de red y de los servicios. Controla la disponibilidad y el acceso a los recursos de portadora, del subsistema y los servicios.

Se comunica con la función de tarifas o tarificación (RF) para determinar el valor de los recursos usados y con la función de gestión de saldo de la cuenta (ABMF) para consultar y actualizar la cuenta del suscriptor y el estado de sus contadores [35].

4.8.4.2.2. Tarificación por sesión (SBCF)

Realiza la tarificación y el control de crédito por sesión en el nivel de portadora, de red y de servicio, es decir, en base a la sesiones de de red. Controla el establecimiento y la finalización de sesiones de en la red,

el acceso a los recursos de las portadoras y la disponibilidad de los servicios [35].

Se comunica con la función de tarifas o tarificación (RF) para determinar el valor de los recursos y las sesiones establecidas y con la función de gestión de saldo de la cuenta (ABMF) para consultar y actualizar la cuenta del suscriptor y el estado de sus contadores.

4.8.4.3. Función de gestión de saldo/balance de la cuenta (ABMF)

Es la función que se encarga de proporcionar el saldo disponible en la cuenta del cliente hacia la subfunciones EBCF y SBCF a través del protocolo Diameter por la interfaz Rc de comunicación.

4.8.4.4. Función de tarificación (RF)

Es la función encargada de determinar cuál es el valor de los recursos de red utilizados. Determina cual es la tarifa o el precio (en unidades monetarias o no) para uno o varios eventos tarificables proporcionados por las subfunciones EBCF y SBCF a través del protocolo Diameter por la interfaz Re. Recibe de ésta un conjunto de parámetros relacionados con el evento de tarificación a valorar, como volumen de datos transmitidos, tiempo de uso del servicio o de los recursos, localización e identificación del usuario, identificador de recursos o servicios usados, etc., a partir de los cuales establece cual será la tarifa o precio a aplicar a cada evento, servicio o sesión establecida [33].

4.8.4.5. Pasarela de comunicación S-CSCF – OCF (IMS GWF)

Una de las entidades indicadas anteriormente que se comunican con el sistema de tarificación online (OCS), la función de control de sesión (S-CSCF) no incorpora la capacidad de activación de recopilación de información de tarificación (CTF) por si misma hacia el sistema de tarificación en tiempo real, si no que conecta a través de la interfaz ISC, utilizando el protocolo de comunicación SIP, con una funcionalidad similar que como si fuera un servidor de aplicación más , solicitará dicha información al control de sesión y la convertirá al protocolo de comunicación de seguridad (Diameter) para transmitirla por la interfaz de comunicación Ro, hacia la función de tarificación online (OCF). En las ilustraciones 27 y 28 se puede observar esta pasarela de conversión, colocada entre el S-CSCF y el OCS.

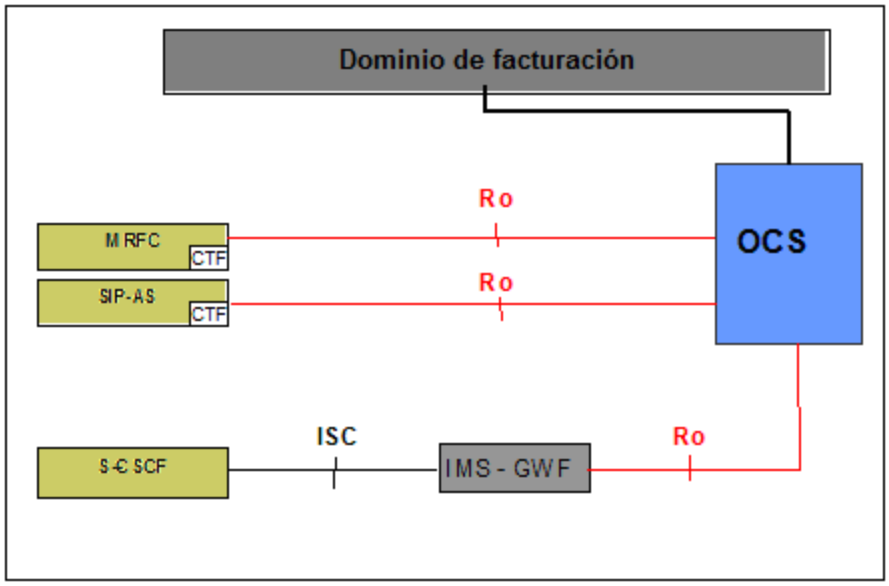

Figura 41. Arquitectura del sistema de tarificación online

5. Procedimientos en la red multimedia

5.1. Introducción

Definidos los principios fundamentales, las características principales, la arquitectura y las entidades funcionales que conforman la red troncal de la red multimedia se hace necesario definir el conjunto de operaciones, procedimientos y reglas que se producen entre entidades para que tenga lugar las comunicaciones entre usuarios y el acceso a los servicios ofrecidos. Para esto detallaremos como son los flujos de señalización entre los diferentes elementos de la red.

5.2. Procedimiento de registro en la red multimedia

Antes de que el usuario pueda hacer uso de los servicios de comunicación de la red multimedia éste tiene que registrarse en la red multimedia a la que pertenece para identificarse y obtener autenticación y autorización de acceso a los servicios ofrecidos por el operador del sistema. Para que esto se produzca el terminal de usuario y la red tienen que seguir una serie de operaciones para satisfacer todas las condiciones necesarias para el registro del usuario.

5.2.1. Establecimiento de conexión con la red de acceso de conectividad IP (IP-CAN)

El primer paso es el establecimiento de una conexión de datos con la red de acceso de conectividad IP por medio de la cual el usuario accede a la red multimedia. Como indicamos en el punto 2.3.4 el nivel de acceso está completamente desligado de la red troncal facilitando el uso de múltiples redes de acceso con conectividad IP, como redes de datos digitales de suscriptor (DSLs), redes corporativas de acceso local (LANs), redes móviles terrestres inalámbricas (GPRS y EPS), redes locales inalámbricas (WLANs), redes de microondas (WiMAX) etc.

Cada red tiene sus propios mecanismos para establecer conexión con el terminal de usuario pero nos vamos a centrar en las redes móviles terrestres y sus redes de acceso de datos, GPRS y EPS y en como proporcionan conectividad IP al terminal de usuario a través de la conexión que establecen con éste, por medio de la activación de un contexto PDP en GPRS o de una conexión PDN en EPS [26].

El terminal de usuario solicita la activación de un contexto PDP o conexión PDN contra el nodo de control en la red de datos, SSGN o MME, que realizará algunas funciones previas a la activación del contexto o conexión con el terminal de usuario, como son identificación del terminal y del suscriptor (realiza tareas de autenticación y autorización en la red de acceso), selección de punto de acceso a la red, identificación de la red a la que se desea conectar, etc. cuando estas tareas están completadas, el SSGN/MME envía la solicitud de activación al GGSN/P-GW adecuado que conectara

con la red multimedia, y proporcionara una dirección IP (IPv4 o IPv6) válida para el contexto o conexión creada.

Para el resto de redes de acceso (LAN, WLAN, DSL, WiMAX, et) el procedimiento más habitual es el uso del protocolo de configuración dinámica (DHCP) que proporciona datos de configuración al terminal, asignación de dirección IP, dirección de servidores de nombre (DNS) u otros parámetros relevantes para el terminal. No entraremos más en detalle de cómo se realizan estos procedimientos al estar fuera del objetivo de estudio de este trabajo.

5.2.2. Detección de P-CSCF

El procedimiento por el cual el terminal de usuario obtiene la dirección IP del punto de contacto dentro de la red multimedia, se puede realizar a través de diferentes mecanismos:

- A través del mecanismo de configuración dinámica del terminal, DHCP, mencionado en el punto anterior, que proporcionará al terminal de usuario (UE) o bien la dirección IP del P-CSCF o el nombre de dominio del P-CSCF y la dirección del servidor de resolución de nombres (DNS) que resolverá el nombre del servidor proporcionado.
- Otro mecanismo es que la obtención de la dirección del P-CSCF durante la activación del contexto PDP/conexión PDN en la red de acceso.
- Otra posibilidad es que el dominio del nombre o la dirección IP del servidor P-CSCF sea conocido desde el comienzo por el terminal de usuario (provisión inicial en la IMSI del suscriptor).

Explicaremos como se obtiene la dirección a partir del primer procedimiento detallado.

5.2.2.1. Obtención de la dirección de P-CSCF a través de DHCP/DNS

Este procedimiento se basa en el uso del protocolo de comunicación DHCP para permitir el envío de los parámetros de configuración desde el servidor de DHCP de la red hacia el terminal de usuario con la ayuda de la red de acceso.

Una vez que el terminal tiene una conexión activa con la red de acceso (IP-CAN) envía una solicitud DHCP a la red de acceso que ésta se encargará de retransmitir hacia un servidor DHCP, que al recibir la petición, responderá con la dirección IP del P-CSCF o con el nombre de dominio del mismo y con la/s dirección/es de los servidores DNS que pueden resolver dicho nombre. Las figuras siguientes muestran este proceso.

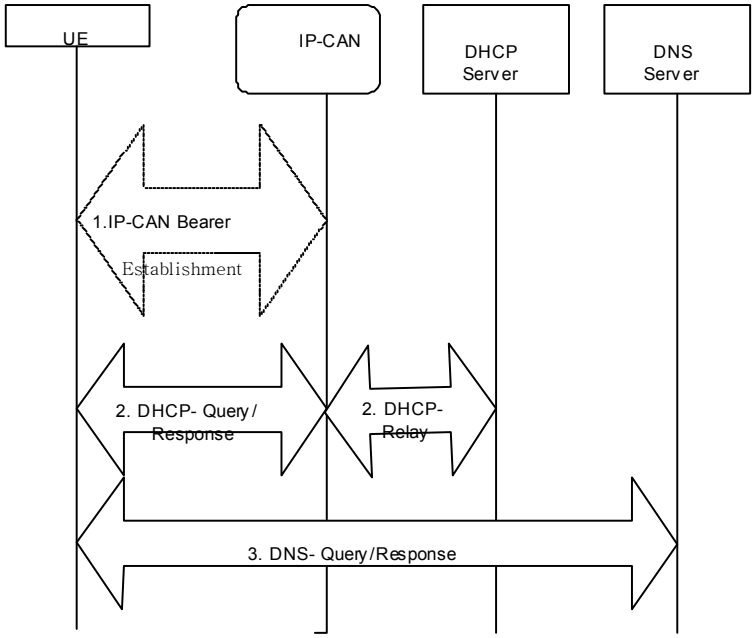

Figura 42. Obtención de la dirección del P-CSCF

En este último caso cuando el terminal reciba estos datos, hará una consulta al DNS proporcionado para resolver el nombre del dominio del P-CSCF y obtener su dirección IP. En esta consulta el terminal primero pregunta al DNS por el protocolo de transporte y el puerto de comunicación, si los desconoce, haciendo una consulta NAPTR al DNS y después resuelve el nombre del dominio completo, haciendo una consulta SRV al DNS [26].

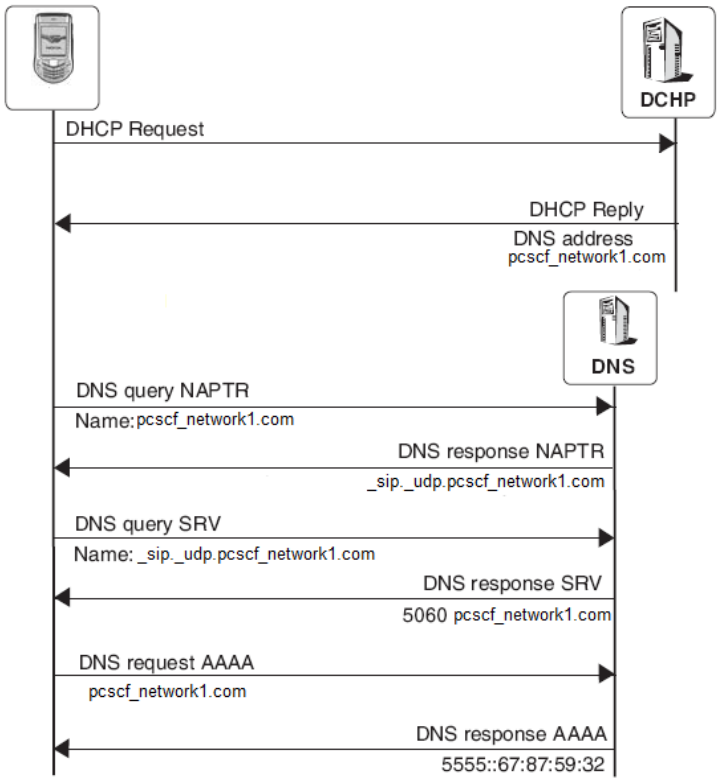

Figura 43. Consultas NAPTR y SRV al DNS por el UE

5.2.3. Localización del usuario y punto de entrada de la red

A partir de este momento el terminal podrá iniciar la comunicación con la red multimedia y comenzará el proceso de registro del terminal en la misma. El terminal de usuario iniciará el registro construyendo y enviando una petición de registro con el mensaje SIP REGISTER al P-CSCF.

Antes de determinar cuál será la entidad de control de la red que realizará el registro del terminal, primeramente, el proxy P-CSCF, determinará si el usuario conectado pertenece al operador de la red a la cual pertenece el P-CSCF, es decir se trata de la red local del usuario, o si por el contrario no pertenece al operador de la red en la que el proxy se encuentra, es decir, el usuario se encuentra en una red en itinerancia o roaming.

Si este último caso se diera, el proxy resolverá a partir del identificador del usuario (URI del usuario) y del dominio de red proporcionados por el ISIM en el terminal, cual es la red local del usuario en cuestión y el punto de entrada en dicha red para las comunicaciones del usuario, el I-CSCF. Para obtener la dirección del I-CSCF al que retransmitirá la solicitud REGISTER, el proxy realiza una consulta a un DNS para determinar la dirección IP, el puerto y el protocolo de transporte con el mecanismo descrito anteriormente (solicitudes NAPTR y SRV al DNS)[26 y 36].La figura 44 ilustra este mecanismo.

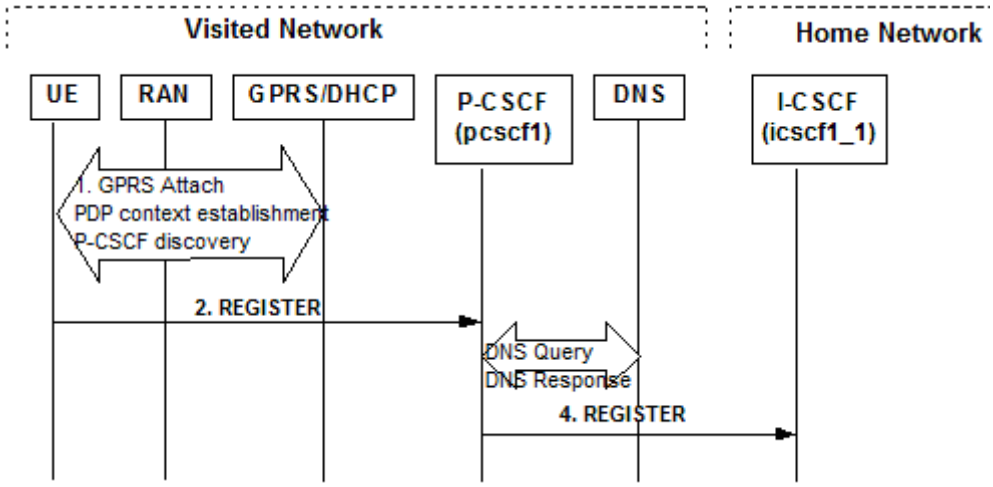

Figura 44. Selección del punto de entrada en la red.

En el caso de que el proxy se encuentre localizado dentro de la red local del usuario, el proceso sería el mismo pero sin salir del dominio de esta red. En los dos escenarios mencionados es necesario localizar el servidor I-CSCF como paso previo a la asignación de la entidad que se encargará del registro del usuario en la red, el S-CSCF.

5.2.4. Asignación de S-CSCF y autenticación del usuario

5.2.4.1. Asignación de S-CSCF

Una vez que el servidor I-CSCF ha recibido la petición SIP REGISTER, empieza el proceso para determinar cuál será el próximo paso dentro de la red. El I-CSCF no es consciente de si el equipo de usuario se encuentra ya registrado o si está ya asignado, por ello envía una solicitud de información del estado de registro de la suscripción del usuario al repositorio principal de datos de la red, el HSS, sobre la interfaz Cx utilizando el comando de autenticación de usuario (UAR) del protocolo Diameter. En dicho comando se indica la identidad privada del usuario, la identidad pública que se pretende registrar, la identificación de la red en la que se encuentra el terminal (en itinerancia o local), obtenidas todas ellas de la petición REGISTER. Al recibir el comando el HSS valida la información recibida y responde con el mensaje de autenticación de usuario (UAA) con información del servidor S-CSCF al que está asignado, si resulta que el usuario ya está registrado en la red o con un conjunto de capacidades para que el I-CSCF realice el proceso de elección de un S-CSCF. Este conjunto de capacidades es la información relevante que necesita conocer el I-CSCF para la elección de servidor para ese usuario concreto como [26]:

- Capacidades necesarias que tiene que tener el S-CSCF para cumplir con los servicios que tiene configurados ese usuario.
- Disponibilidad de los servidores de la red, información de carga de cada uno, etc.
- Información de donde está localizado el usuario.
- Preferencias del operador, definidas en las reglas de política de uso.

El I-CSCF contiene una tabla con toda la información de capacidades de cada S-CSCF en la red y en base a esta y a la información recibida en la respuesta UAA realiza una elección.

Cuando el S-CSCF ya ha sido elegido el I-CSCF retransmite la solicitud REGISTER al primero. La ilustración 31 muestra este procedimiento.

5.2.4.2. Autenticación del usuario

A la recepción de la petición de registro, el S-CSCF deberá autenticar al usuario para permitir su registro y su acceso a los servicios de la red. Si la petición llega sin protección de integridad desde el P-CSCF, entonces el S-CSCF tendrá que solicitar información al usuario para autenticarlo. Para ello, el S-CSCF contactará y descargará la información de autenticación de ese usuario desde el HSS en base a la identidad privada recibida (cuyo único propósito es ser utilizada en la autenticación) y construirá el vector de autenticación, que será la

estructura que utilizará para validar al usuario. Este vector se basa en el mecanismo de autenticación servidor-cliente denominado AKA para los terminales que soportan módulos con información del cliente (ISIM, USIM, SIM etc.…) explicado en el punto 3.2.4.4, y tendrá la forma:

AV = RAND||AUTN||XRES||CK||IK [24]

El S-CSCF con la información descargada construirá una respuesta para el terminal de usuario que incluirá una secuencia codificada en base64 de los parámetros RAND y AUTN e información específica del servidor, incluirá los parámetros CK e IK para el P-CSCF y almacenará el resto de los parámetros del vector. Este mensaje de respuesta será un mensaje de error SIP: 401 (Unauthorized) rechazando el registro solicitado por el terminal de usuario. Puesto que la estructura de seguridad empleado por SIP es SIP Digest, al enviar la respuesta hacia el terminal de usuario, será necesario hacer un mapeo de los parámetros AKA sobre las cabeceras de autenticación de SIP [21]:

```
SIP/2.0 401 Unauthorized
WWW-Authenticate: Digest realm="home.com",
nonce=A34Cm+Fva37UYWpGNB34JP, algorithm=AKAv1-MD5,
Ik="0123456789abcdeedcba9876543210",
Ck="9876543210abcdeedcba0123456789"
```

El campo nonce transporta en una codificación base 64 los parámetros RAND, AUTN e información del servidor adicional.

La figura 45 ilustra la respuesta hacia el terminal del usuario.

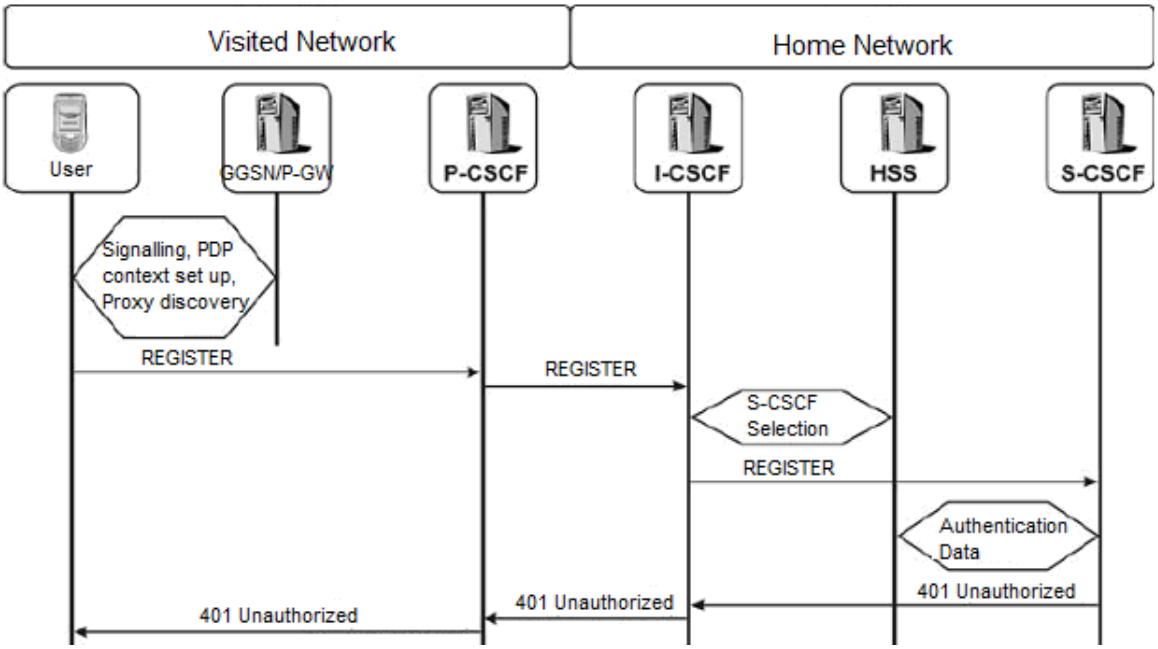

Figura 45. Selección de C-CSCF y autenticación del usuario

5.2.5. Generación de claves de sesión y autenticación en el usuario

A la recepción de la respuesta del intento de registro 401 (Unauthorized), el terminal extrae los parámetros relativos a credenciales que tendrá almacenados en el módulo USIM/ISIM (que en el caso de los terminales móviles se encuentran almacenado en la tarjeta UICC), que será la clave compartida K y el numero de secuencia SQN y validará a la red (extrae el parámetro MAC del recibido AUTN y lo compara con parámetro calculado XMAC y si coinciden y SQN está bien, valida a la red) y generará la respuesta para la red RES (con sus parámetros y el código RAND recibido) y las claves para la sesión, IK y CK.

Cuando el terminal tiene preparada la respuesta con los parámetros de autenticación, los incorpora en los campos correspondientes de la cabecera SIP de una nueva petición SIP REGISTER que enviará nuevamente a la red.

Puesto que todavía el terminal no ha aprendido cual será el servidor que controla el proceso de registro repite los procedimientos desarrollados en los puntos 5.2.3 y 5.2.4. En la siguiente figura se ilustra el proceso.

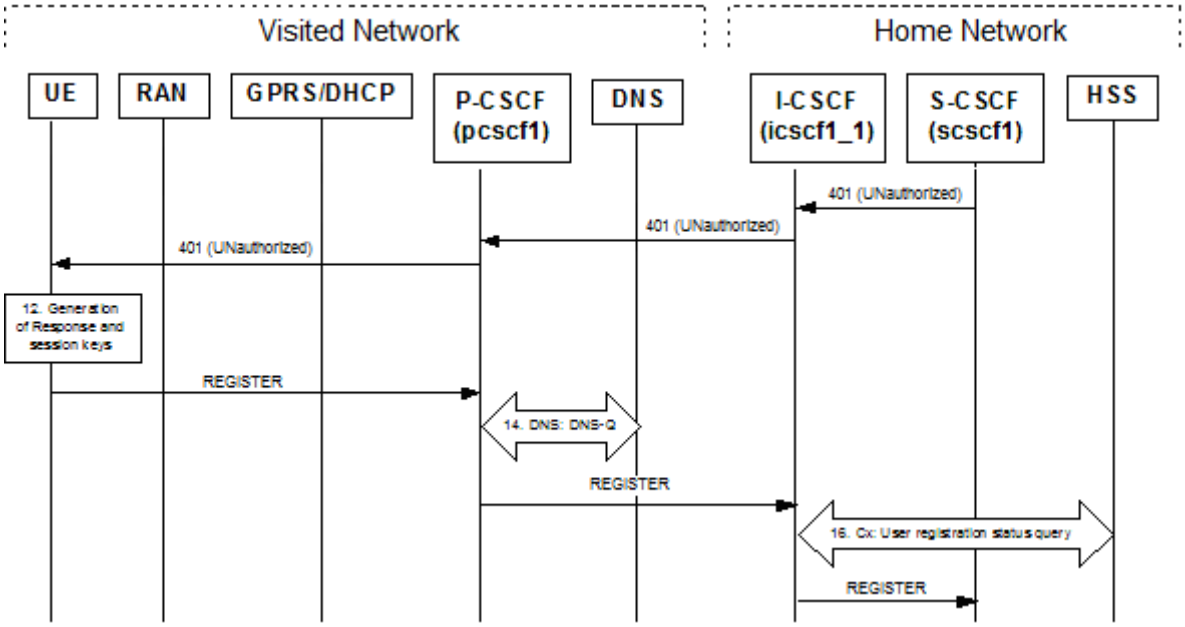

Figura 46. Respuesta por parte del UE y envío de petición de registro

5.2.5.1. Asociación de seguridad entre el P-CSCF y UE

Durante el proceso de autenticación entre la red (S-CSCF) y el terminal de usuario tiene lugar el establecimiento de la asociación de seguridad entre el usuario y su primer punto de comunicación en la red, el P-CSCF. Esta asociación de seguridad tiene como finalidad el establecimiento de una comunicación segura entre ambos extremos para el intercambio de mensajes de señalización después de negociar y acordar el conjunto de parámetros y puertos de seguridad que serán usados. Estas asociaciones de seguridad, que se realizan sobre la estructura indicada en el punto 3.2.4.3.2, IPsec, se validan a través de una clave

compartida por ambos extremos. Esta clave compartida, será el parámetro IK del vector de autenticación de AKA. El P-CSCF recibirá las claves de la sesión IK y CK en la respuesta 401 (Unauthorized) a la primera petición de registro enviada por el terminal y el UE generará las claves en su respuesta al proceso de autenticación iniciado por la red. Al coincidir esta clave de sesión, el P-CSCF y el UE establecerán dos pares de asociación de seguridad sobre IPsec para su comunicación, donde cada uno asigna una conexión lógica y un puerto para el envío de mensajes y otra equivalente para la recepción de mensajes. En la siguiente ilustración se muestra el establecimiento de las asociaciones de seguridad entre la red y el terminal [21].

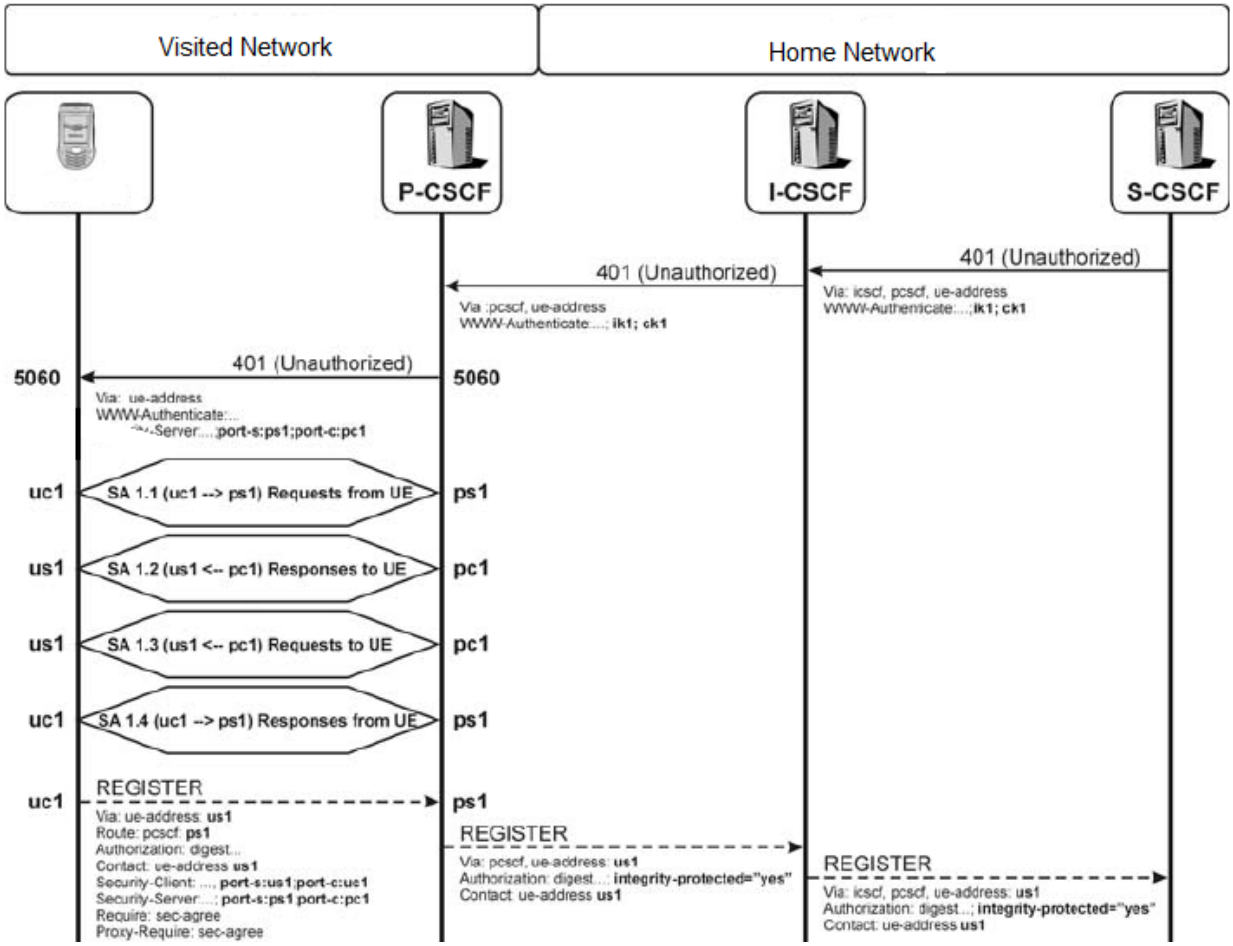

Figura 47. Negociación de SA entre el P-CSCF y UE

5.2.6. Autenticación y registro del usuario en la red

En este segundo intento, el S-CSCF recibe la respuesta bajo condiciones de protección de integridad (IK) y compara la respuesta generada por el terminal de usuario RES, con la respuesta esperada XRES que mantenía almacenada. Cuando estos coinciden, el S-CSCF autentica al usuario en la red multimedia y registra la identidad publica de usuario proporcionada. A continuación el S-CSCF notifica que el usuario ha sido registrado en esa entidad de control al HSS que responderá al C-CSCF

permitiéndole descargar la información del perfil del usuario registrado. El perfil de usuario contendrá entre otros, las identidades de públicas de usuario asociadas con la identidad privada registrada o información de activación de servicios, que es una colección de eventos para determinar cuándo una petición SIP es enviada a un servidor de aplicación (AS).

Finalmente el S-CSCF notificará al usuario que ha sido correctamente registrado en la red multimedia a través de la respuesta SIP 200 OK. Esta respuesta se propagara por el camino establecido para que los elementos de red registren la información de necesaria para recordar el camino de señalización para posteriores comunicaciones entre el usuario y el control de sesión. Si algún elemento del camino de señalización establecido no requiere permanecer en el mismo, no incluirá su dirección en el campo de cabecera *Record-Route* para que las entidades adyacentes no almacenen su dirección y no la incluyan en las peticiones y respuestas siguientes. La figura 48 muestras los procesos detallados en este punto.

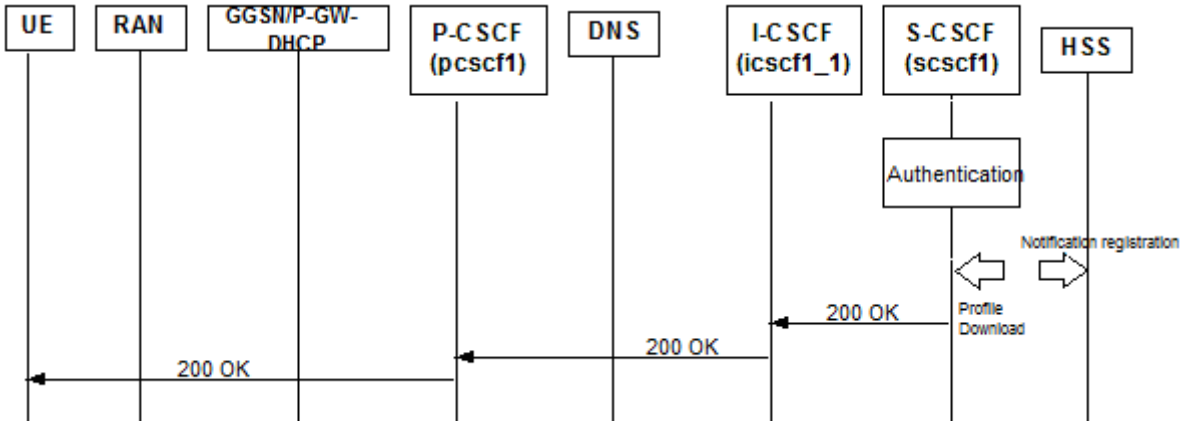

Figura 48. Autenticación, descarga del perfil y notificación al usuario del registro

5.2.7. SIP Digest

Como estructura de seguridad destinada a redes de acceso diferentes a las redes de acceso definidas en las especificaciones de 3GPP donde el terminal de usuario no soporta el mecanismo IMS-AKA se emplea el método de seguridad nativo de SIP basado en el mecanismo HTTP Digest [38] donde el usuario y la red comparten una contraseña o clave preestablecida y asociada con la identidad privada de usuario que es la que autenticará al suscriptor como comentamos en el punto 3.2.4.5.1.

El proceso de autenticación comienza cuando el servidor de control de la sesión recibe una petición de acceso y responde interrogando al terminal de usuario para que éste se autentifique. El servidor genera para ello una secuencia encriptada con el algoritmo MD5 en base 64 conocida como `nonce` que solo será utilizado en la autenticación a partir de una secuencia aleatoria generada por el servidor y una clave privada que solo conoce el servidor:

```
Nonce= base64 (secuencia aleatoria: clave privada)
```

Que retransmitirá al usuario junto con el nombre del dominio al que pertenece el servidor, el tipo de protección requerida (opcional), el URI proporcionado por el usuario en el campo Request-URI de la petición y el algoritmo de autenticación utilizado para generar el `nonce`:

```
SIP/2.0 401 Unauthorized
WWW-Authenticate: Digest, realm="home.com",
qop="auth o auth-int", digest_URI="Request-URI"
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093", algorithm="MD5"
```

Cuando el terminal de usuario recibe el mensaje, genera una respuesta donde incluye entre otros parámetros una secuencia hash llamada `response` calculada en base 64 con el algoritmo MD5 a partir de los datos proporcionados por el servidor en el campo `WWW-Authenticate`, el nombre de usuario y la contraseña de la identidad privada que se quiere autenticar e incluso el cuerpo del mensaje SIP (si lo hubiese):

```
Response: base64(realm:qop:digest-URI:nonce:user:password:SIP_Body)
```

Que junto con algunos de estos parámetros (excepto la clave compartida) son enviados como respuesta hacia el servidor. Éste cuando recibe la respuesta con todos los parámetros calcula nuevamente el hash en base a los mismos parámetros de entrada que utilizo el cliente pero usando su propia clave compartida almacenada. Si ambas funciones dan el mismo resultado entonces el servidor considera como autenticado al terminal de usuario y le permite acceso a la red [18, 38 y 39].La siguiente figura muestra un ejemplo de este método

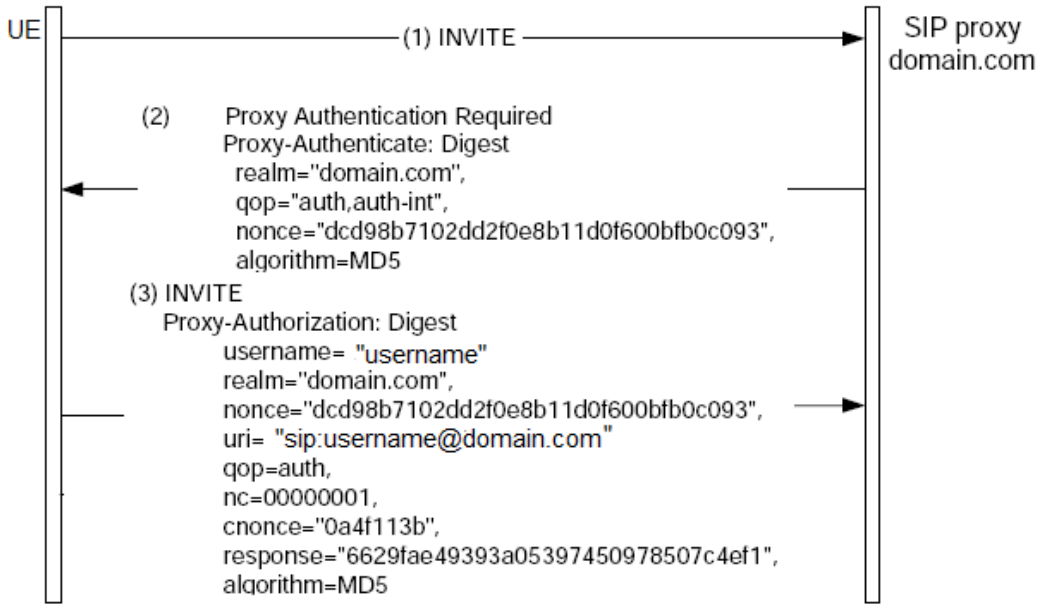

Figura 49. Ejemplo de autenticación utilizando el mecanismo SIP Digest.

5.2.8. Suscripción a los eventos de estado de registro

A partir del momento en el que se produce el registro en la red, ésta se encarga de llevar un control del estado del registro del usuario. Puede ser interesante que diferentes entidades de red o el propio terminal de usuario tengan constancia de si se producen cambios en el estado del registro por medio de la suscripción a eventos de estado. Este mecanismo permite que en caso de que se produzca alguna modificación en el estado de registro, si el terminal se desregistrase, si fuera necesario un re-registro o re-autenticación de la identidad privada del usuario, si se produjera algún fallo en la red que obligase a desvincular al terminal de ésta por poner algunos ejemplos, todas aquellas entidades que estuvieran suscritas a las notificaciones de eventos, serán informadas y podrán tomar las medidas necesarias (el terminal inicia algún procedimiento, informa al usuario, liberar recursos o elimina asociaciones de seguridad, etc.)

El terminal o entidad en cuestión, enviará una petición SIP SUSBCRIBE relativa a la entidad de usuario pública registrada por el nodo de gestión, S-CSCF, a través del camino de señalización que se ha establecido durante el proceso de registro inicial. La red recibe la petición y activa las notificaciones para esa entidad, en este caso el terminal de usuario, y responde con el mensaje SIP 200 OK a la petición SUSCRIBE para confirmar que la petición ha sido activada. La red a continuación envía una notificación SIP NOTIFY al UE, por el cual proporciona información adicional al terminal de todas las identidades públicas del usuario y del estado de registro de cada una de ellas.

Si se produjeran posteriores cambio el S-CSCF informará utilizando nuevamente el método NOTIFY a lo que el terminal contestará con un mensaje de respuesta dándose por informado. La siguiente ilustración muestra el flujo establecido [36].

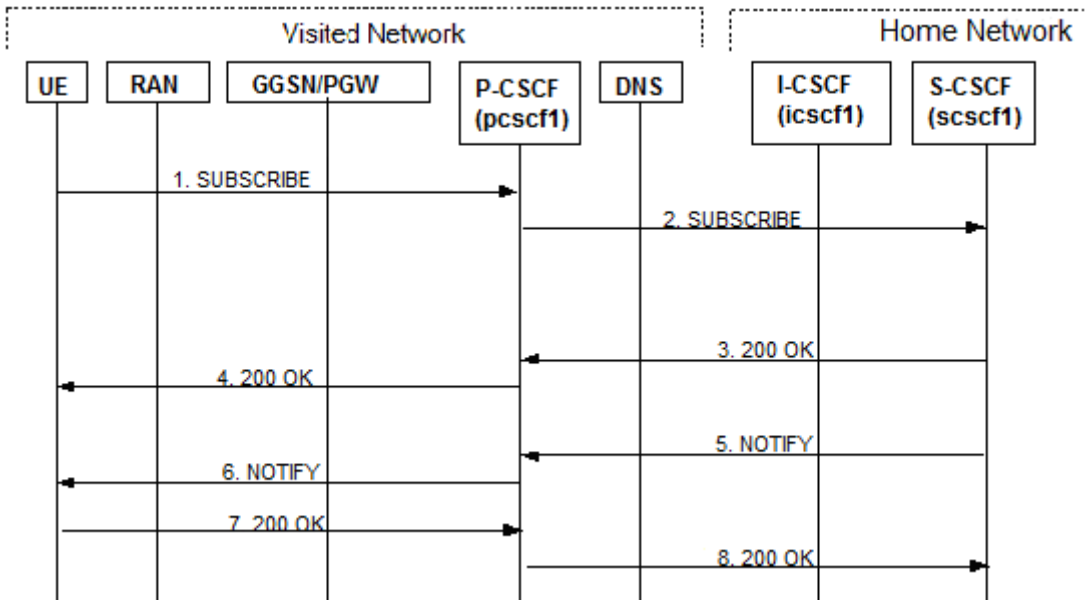

Figura 50. Suscripción a notificación de estado por UE

El proceso que hemos indicado previamente puede realizarse además de por el terminal de usuario por otras entidades de red, como el P-CSCF o algunos AS, que pueden requerir información del estado del usuario para realizar acciones asociadas a la información recibida, por ejemplo si el usuario se desregistra, el P-CSCF elimina la conexión establecida con el usuario y libera los recursos asignados, etc.

5.3. Procedimiento de re-registro en la red multimedia

Es el procedimiento por el cual un terminal de usuario actualiza su conexión a la red, re-registrando la misma identidad pública que tenia registrada anteriormente y actualizando el tiempo de vida del registro anterior. Este mecanismo permite renovar las conexiones a la red en el tiempo. Por otro lado si un terminal que se encuentra registrado en la red alcanza el tiempo máximo de un registro sin registrarse nuevamente, entonces la red dará por expirada y finalizará la conexión.

5.3.1. Iniciado por el terminal de usuario

En el caso de que el mecanismo de actualización de registro en la red sea ejecutado por iniciativa del terminal de usuario cuando el tiempo de expiración de una conexión activa está próxima a finalizar o ha tenido lugar algún cambio en la conexión a la red de acceso, por ejemplo el cambio de la dirección IP asignado por la red de acceso, o en el propio terminal, se sigue el mismo procedimiento que el realizado por el registro inicial en la red de punto 5.2 con algunas consideraciones. A diferencia de la solicitud inicial, el terminal utiliza las conexiones de seguridad que fueron establecidas en la parte final del proceso de registro inicial, por lo tanto, la petición REGISTER, llega a la entidad de control S-CSCF, con el mecanismo de protección de integridad activado, lo que significa que la red sabe que la petición viene de un origen que ya está verificado y no tiene que requerir nuevamente sus credenciales para autenticarlo. En este proceso, la red solo refresca el tiempo de registro actual con el tiempo solicitado por el terminal de usuario siempre que la política de red lo permita.

En la figura 51 se muestra como el proceso es análogo al del punto 5.2 pero sin incluir el proceso de autenticación del usuario lo que lleva a que el proceso de re-registro sea más breve y más simple que el registro inicial.

5.3.2. Iniciado por la red

La activación del mecanismo de re-registro también puede ser solicitada por la red, debido a un cambio en el estado de registro del usuario producido por un cambio en la propia red, un cambio en la política del operador o la solicitud de la red de re-autenticar al usuario nuevamente, a través del envío de la correspondiente notificación a las entidades suscritas a la notificación de eventos expuesta en el punto 5.2.7. Esta notificación indicará que la conexión actual se modifica en un sentido que fuerza al terminal de usuario a responder con una nueva solicitud de registro en la red.

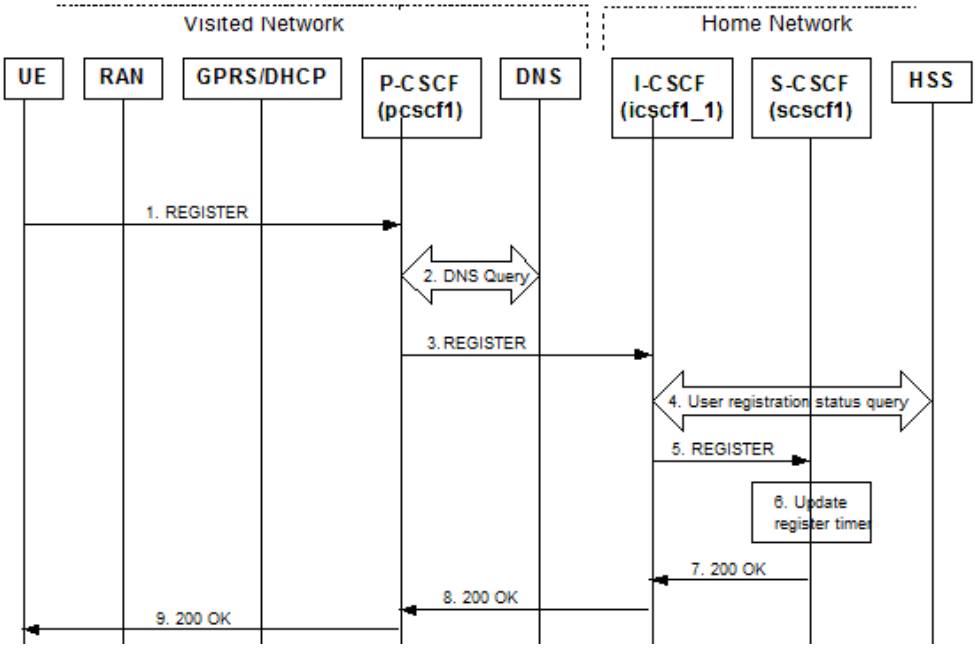

Figura 51. Proceso de re-registro en la red multimedia

5.4. Procedimiento de desregistro en la red multimedia

Es el procedimiento seguido para desregistrar entidades públicas de usuarios que están registradas en la red, bien por iniciativa del terminal de usuario o bien por indicación de la red multimedia a través de diferentes mecanismos.

5.4.1. Iniciado por el usuario

El usuario o el terminal de usuario puede requerir en algunas situaciones desregistrarse de la red a través del envío de una nueva solicitud SIP REGISTER donde el valor del campo de tiempo de expiración es puesto a cero segundos lo que permitirá que la identidad pública de usuario se desvincule de la dirección IP que tiene asignada el terminal en ese momento. El procedimiento sigue el flujo detallado para el registro inicial en la red, a través del P-CSCF se determina el I-CSCF local y éste pregunta al HSS si conoce que entidad controla al usuario.

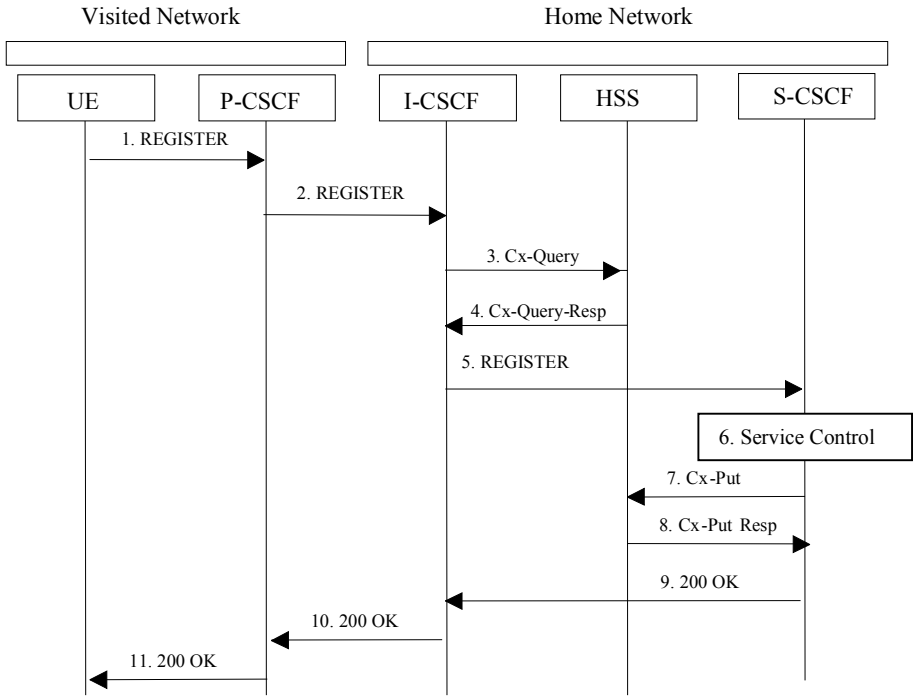

Figura 52. Desregistro en la red solicitado por el UE

Cuando la solicitud llega al S-CSCF que controla al terminal, éste realizará las operaciones para desregistrar al usuario, como actualizar como no registradas las identidades públicas del usuario en el HSS, desvincular la dirección IP del terminal de la identidad registrada, informar al nivel de servicio si procediera etc. Cuando el proceso haya finalizado el S-CSCF notificará con la respuesta SIP 200 OK al terminal que el desregistro ha finalizado con éxito. Si el terminal u otras entidades estuvieran suscritos al servicio de notificación de evento, el S-CSCF enviará una solicitud SIP NOTIFY indicando que dicha entidad ya no está registrada y finalizando la suscripción de información para ese usuario [26].

5.4.2. Iniciado por la red

El proceso de desregistro también puede ser iniciado por las entidades de red y puede atender a diferentes motivos [26]:

- Por cuestiones de gestión de tráfico o de red, si se produce la caída de un nodo o de una parte de la red o si el volumen de tráfico pone en riesgo la estabilidad de un nodo o elemento de la red.
- Si hay una pérdida de conexión o no hay respuesta, por parte del terminal o con la red de acceso, como una pérdida de cobertura, apagado inesperado del terminal, etc.
- Por cuestiones de eficiencia, como evitar que un usuario de red esté registrado dos veces.

- Por cuestiones de mantenimiento de red. Debido a trabajos de mantenimiento en la red, el operador puede forzar a cancelar el registro de usuarios en la red.
- Por cuestiones administrativas, como extinción del contrato o de la suscripción en la red, control de fraude etc.

Dependiendo del motivo que lleva a la red a desregistrar a un usuario, este será iniciado por el control de la sesión (S-CSCF), por el control de la suscripción (HSS) o por el control del servicio (AS). Son dos los mecanismos utilizados por la red para desregistrar un usuario son:

- Agotar el tiempo de expiración del registro del usuario, no permitiendo que el usuario se re-registre en la red.
- Forzar explícitamente el desregistro del usuario.

5.4.2.1. Desregistro en el nivel de control

En este caso el nivel de control inicia el desregistro de la identidad pública del usuario registrada por cuestiones de eficiencia y gestión de tráfico en la red (mantenimiento, estabilidad de la red, etc.), perdida de conexión (perdida de cobertura o apagado inesperado del terminal, etc.) u otros. El S-CSCF envía una notificación del evento informando de que el registro de la identidad ha sido "terminado" a todas las entidades suscritas a información de estado, incluido el terminal de usuario, finalizando el registro y la suscripción a tal evento.

El S-CSCF aplica inmediatamente las acciones necesarias para restringir el acceso a los servicios de la red y actualiza el estado de registro del usuario en la base de datos de la red.

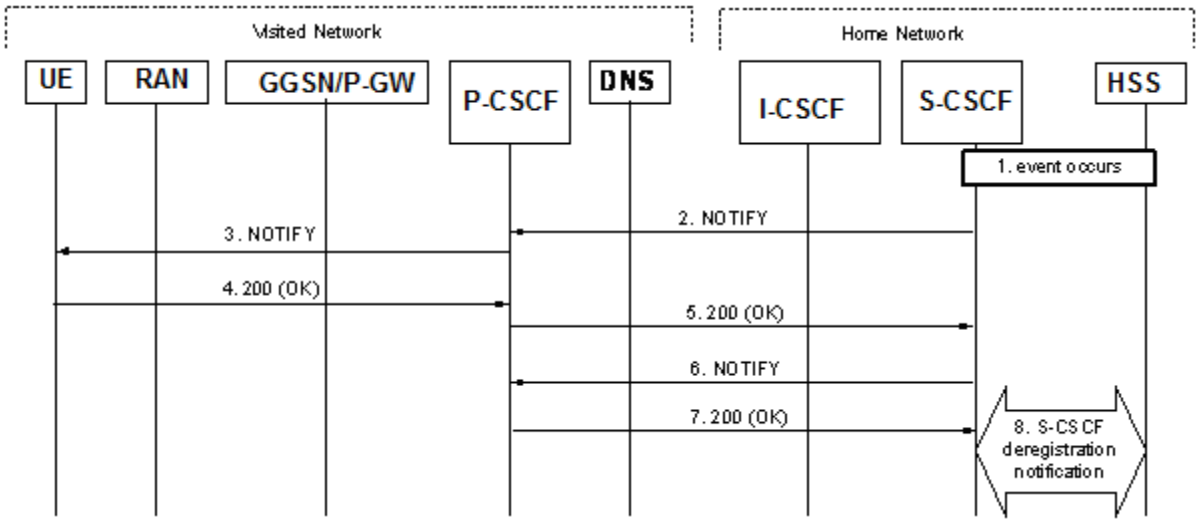

Figura 53. Desregistro iniciado por el nivel de control

5.4.2.2. Desregistro en el nivel administrativo

El proceso puede también ser iniciado por un evento ocurrido en el nivel administrativo, es decir, por un cambio en la suscripción del cliente a los servicios del operador, modificación de la información de suscripción, cancelación de la suscripción del usuario, etc.

Es el HSS el que advierte de los cambios administrativos y lo solicita al control S-CSCF, para que éste notifique al terminal de usuario y a todas las entidades de red, suscritas a la notificación de eventos, que la identidad pública del usuario ya no está registrada y finalice todas las suscripciones a eventos para dicho usuario. Finalmente el S-CSCF responde la solicitud de desregistro realizada por el nivel administrativo, actualizando la información del estado de la/s identidad/es pública/s del usuario. El siguiente diagrama ilustra el flujo que tiene lugar para este procedimiento.

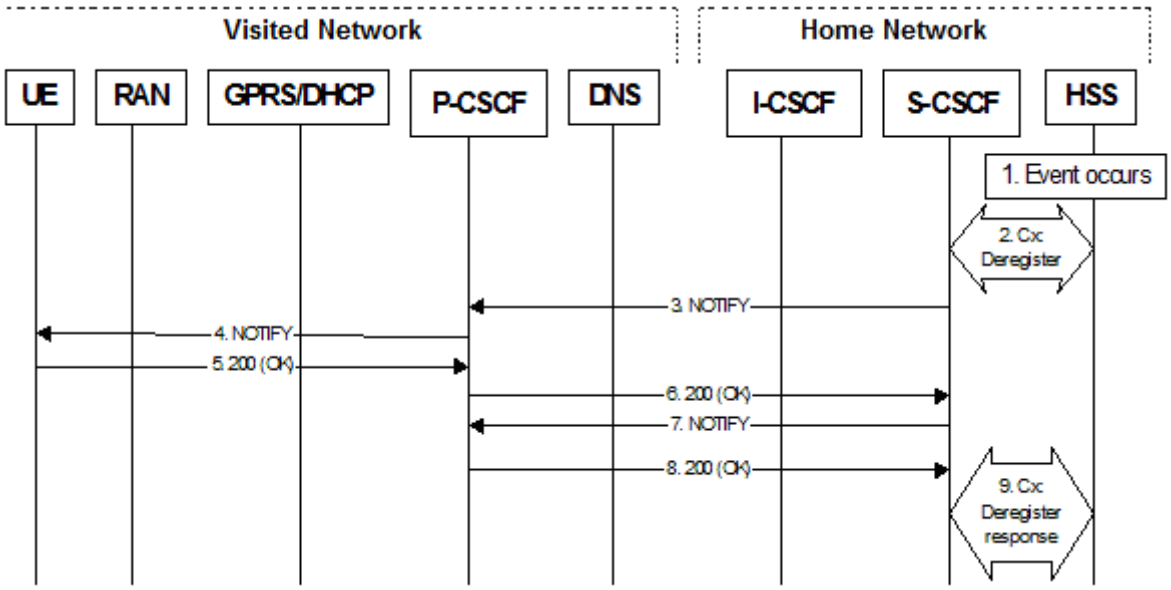

Figura 54. Desregistro iniciado por el HSS

5.4.2.3. Desregistro en el nivel de servicio

Análogo a los dos casos anteriores, el nivel de servicio también puede solicitar al nivel de control el desregistro de la/s identidad/es pública/s de un usuario. Este procedimiento sigue el flujograma de la ilustración siguiente.

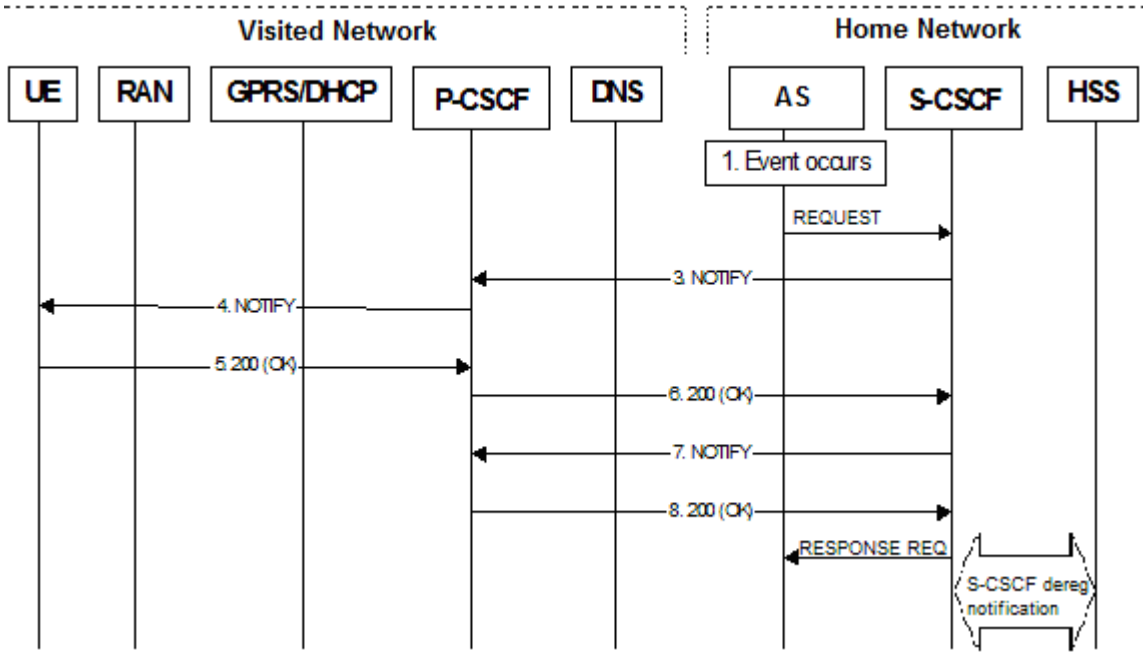

Figura 55. Desregistro solicitado por el nivel de servicio.

5.4.2.4. Notificación de desregistro

A continuación se detalla un ejemplo de cómo sería el mensaje de notificación enviado por el nivel de control del usuario a todas las entidades, incluida el terminal de usuario, suscritas a la notificación de eventos para esa/s identidad/es pública/s de usuario. En el caso de que el usuario sólo tuviera una identidad publica asociada registrada asociada con el mismo perfil de cliente, se añadiría solo información de terminación para esa identidad.

```
NOTIFY sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net;lr>
From: <sip:user1_public1@home1.net>;tag=151170
To: <sip:user1_public1@home1.net>;tag=31415
Call-ID: b89rjhnedlrfjflslj40a222
CSeq: 43 NOTIFY
Subscription-State: terminated
Event: reg
Content-Type: application/reginfo+xml
Contact: <sip:scscf1.home1.net>
Content-Length: (...)

<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
          version="1" state="full">
   <registration aor="sip:user1_public1@home1.net" id="as9"
            state="terminated">
     <contact id="76" state="terminated" event="deactivated">
       <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
     </contact>
   </registration>
 <registration aor="sip:user1_public2@home1.net" id="as10"
            state="terminated">
     <contact id="77" state="terminated"
event="deactivated">
       <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
     </contact>
```

```
</registration>
<registration aor="tel:+358504821437" id="as11"
        state="terminated">
  <contact id="78" state="terminated"
event="deactivated">
      <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
  </contact>
</registration>
</reginfo>
```

5.5. Procedimiento de inicio de sesión multimedia

5.5.1. Introducción

Una vez que se ha producido el registro del usuario, de una o varias identidades públicas, en la red, el usuario está listo para iniciar el uso de los servicios disponibles y establecer sesiones multimedia con otros usuarios de la red o de otros dominios. Antes de que el usuario pueda iniciar el establecimiento de una sesión multimedia tienen que darse algunas condiciones o realizarse algunos procedimientos previos para el correcto funcionamiento de la red.

5.5.2. Determinación del recorrido o camino de señalización

Durante el proceso de registro de un usuario en la red se produce el establecimiento del camino que seguirá la señalización entre el usuario y la propia red para las comunicaciones posteriores al proceso de registro. Este camino se determina al almacenar los diferentes nodos o entidades las direcciones de las entidades a las que enviarán o de las que recibirán mensajes de señalización.

El terminal de usuario almacenará la dirección del P-CSCF, puesto que todas las comunicaciones con la red del usuario se realizarán a través del mismo P-CSCF que controlará que la comunicación cumpla todas las condiciones necesarias. También almacenará la dirección del S-CSCF que gestionará todas las solicitudes desde y hacia el usuario.

Las entidades también almacenarán la dirección de otras entidades en sus bases de datos internas y vincularán estas direcciones a las comunicaciones con un usuario determinado. Para que una entidad permanezca en el camino para sucesivas comunicaciones tiene que añadir su dirección o su nombre a la cabecera *Path* durante el proceso de registro del usuario:

```
REGISTER sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
P-Access-Network-Info:
```

Path: <sip:term@pcscf1.visited1.net;lr>
Require: path
P-Visited-Network-ID: "Visited Network Number 1"
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Contact:
Call-ID:
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net", nonce=base64(RAND + AUTN + server specific data), algorithm=AKAv1-MD5, uri="sip:registrar.home1.net", response="6629fae49393a05397450978507c4ef1", integrity-protected="yes"
CSeq:
Supported:
Content-Length:

En este ejemplo de mensaje de señalización enviado desde el I-CSCF hacia el S-CSCF se indica que el I-CSCF no desea mantenerse en el camino de señalización al no incluir su dirección en la cabecera *path*.

5.5.3. Compresión de la señalización

La compresión de los mensajes de señalización como comentamos en el apartado 3.2.12, es una funcionalidad importante de las redes multimedia ya que el elevado número y el gran tamaño de los mensajes de señalización intercambiados entre el terminal de usuario, UE, y la red, P-CSCF, hace que sea necesario un uso eficiente de los recursos para evitar retrasos significativos en el momento de establecer una sesión multimedia con otros usuarios.

Para lograr esto se utiliza el mecanismo de compresión sigcomp (acrónimo de signalling compression en inglés) descrito en la RFC del IETF 3320. Sin entrar en detalles, este mecanismo realiza una compresión basada en el uso de algoritmos de compresión, donde expresiones o valores grandes son referenciados por punteros o señalizadores pequeños. Este algoritmo es enviado por la entidad compresora del mensaje a la entidad descompresora, permitiendo recuperar los mensajes originales fácilmente y dando flexibilidad a las entidades al elegir el algoritmo de compresión más adecuado para cada situación.

Cuando el terminal de usuario quiere enviar un mensaje de señalización a la red, añade la descripción **comp=sigcomp** en el campo de la cabecera SIP, *contact*, donde indica que está dispuesto a recibir las siguientes peticiones dentro de ese diálogo comprimidas. Si lo indica en el campo *Vía* indica que está dispuesto a recibir todas las respuestas posteriores asociadas a esa petición, comprimidas también.

Por parte del proxy ocurre lo mismo al indicar la descripción **comp=sigcomp** en los campos *Record-Route* y *Vía* respectivamente. Los dos siguientes mensajes de señalización ilustran como sería la petición de sesión INVITE una vez que el terminal ya está registrado en la red y la respuesta provisional enviada por el P-CSCF al UE:

INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp
branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>

P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Supported: 100rel
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-c=8642; port-s=7531
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>

Y en la respuesta del proxy al terminal:

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.visited2.net;lr>, <sip:scscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>,
<sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>

5.5.4. Capacidades y preferencia del terminal de usuario

En el momento de establecerse una sesión multimedia es importante determinar las capacidades de las que dispone el terminal y las preferencias de cada usuario para la sesión, puesto que en base a éstas se producirá la selección de características que definirán la sesión que proporcionará los servicios solicitados por los usuarios.
Antes de aceptar y establecer una sesión el usuario debe ser capaz de indicar cuáles son los parámetros con los que desea establecer una sesión con otro usuario y deberá entablar una negociación con el usuario de destino para acordar cuales serán los parámetros a utilizar en la sesión. Estos parámetros pueden ser:

- Tipos de medios a utilizar en la sesión, como video, audio, texto etc.
- Selección de codificaciones soportadas por cada terminal para cada tipo de medio solicitado.
- Determinación de calidad del servicio. Dependiendo de las necesidades de cada usuario se pueden establecer diferentes niveles de calidad para cada medio requerido.

Para el establecimiento de la sesión por tanto, se tiene que acordar entre ambos extremos de la comunicación cuales serán los medios a utilizar, que recursos proporcionarán dichos medios y en qué condiciones de calidad se proporcionaran estos medios.

5.5.5. Precondiciones de la sesión

Es el mecanismo por el cual la sesión de llamada no se establecerá hasta que los participantes de una sesión multimedia no hayan acordado que clase de sesión y en qué condiciones se establecerá la sesión (negociación de medios) y

se hayan reservado los recursos suficientes tanto en la red de acceso como en la red troncal para su cumplimiento (reserva de recursos).

Para que el conjunto de precondiciones se cumplan tiene que darse:

- Que se negocie y se acuerde un conjunto de medios por los usuarios de la sesión.
- Que se negocie y se acuerde un conjunto de recursos que soportarán la comunicación de cada medio por los usuarios.
- Negociación y acuerdo de calidad mínima de servicio con la que se tiene que proporcionar la sesión.
- Confirmación de reserva de recursos comprometidos por los terminales de usuario en las redes de acceso.
- Confirmación de reserva de recursos en la red troncal (reserva de recursos en el MRFC).

Una vez que el conjunto de precondiciones están satisfechas por ambos extremos, la sesión puede proceder a su establecimiento.

5.5.6. Negociación de medios

Es el procedimiento por el cual se produce una negociación de las características de los medios, incluidos las codificaciones especificas para cada medio, para el establecimiento de la comunicación. El proceso de negociación de medios y codificaciones no sólo se produce previamente al establecimiento de una sesión multimedia sino que puede realizarse durante el transcurso una sesión ya establecida al requerir alguno de los participantes una modificación en los medios o los códec utilizados dentro de la sesión (añadir/eliminar un medio, modificar las características existentes como códec usados, etc.).

Esta negociación es realizada por el intercambio de mensajes donde el usuario solicita todos los medios que desea utilizar en la sesión y las características de éstos (codificaciones soportadas, calidad del servicio, etc.) que soporta. Cuando el mensaje llega al destinatario este responde con otro mensaje indicando cuales de esos medios y que características soportará para esa sesión, asignando un puerto a cada medio aceptado e incluyendo los códec soportados en común con el otro extremo. Cuando el usuario que inicia la negociación recibe la respuesta del destinatario, elegirá el subconjunto de medios y recursos soportados por el destinatario que mejor se ajustan con las preferencia indicadas por el usuario inicial o propondrá otros diferentes si no fueran válidos y los enviará en un nuevo mensaje al destinatario para que éste los confirme o los modifique. El proceso de intercambio de mensajes continúa hasta que el conjunto de medios y recursos es aceptado por ambas partes.

La red se encarga de controlar que todo el proceso está sujeto a la política del operador/es y a los perfiles de cada usuario (permitiendo el uso de medios a los que el cliente está suscrito). La figura 55 representa un ejemplo de cómo se produce esta negociación.

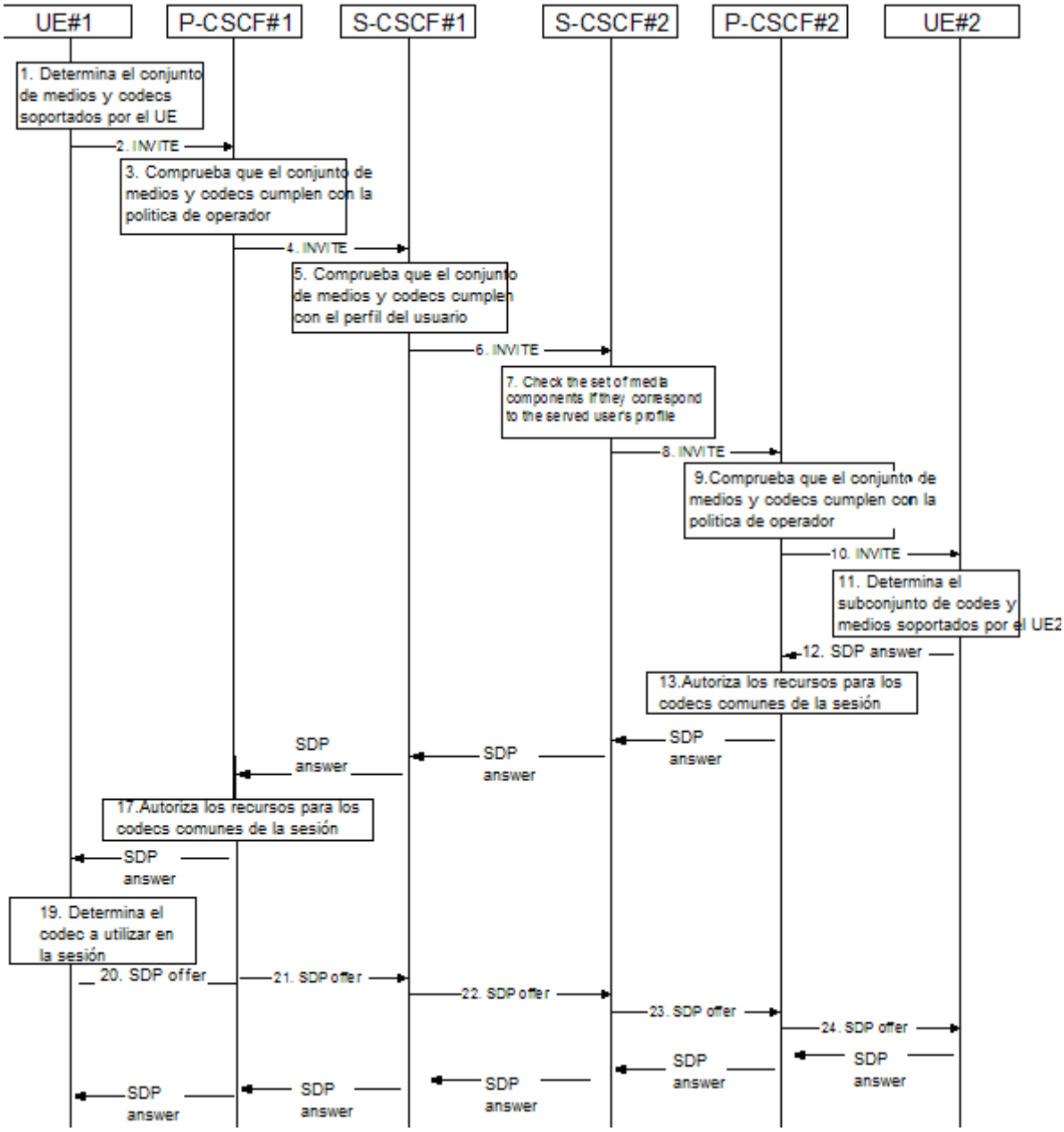

Figura 56. Negociación de medios entres usuarios.

5.5.6.1. Estructura de los mensajes de negociación

El mecanismo utilizado para la descripción de las características de la sesión, es el método de oferta/respuesta nativo de SIP, SDP, por el cual dos o más entidades negocian las características de una sesión multimedia. Los mensajes SDP se transmiten dentro del cuerpo de los mensajes de señalización SIP enviados por el nivel de señalización.

El cuerpo de estos mensajes indican tanto el conjunto de medios que se desean utilizar (líneas m), como las codificaciones soportadas que codifican cada uno de los medio (líneas a), los requisitos de ancho de banda de cada medio (líneas b) y otras características auxiliares. Estos mensajes también los mensajes

relativos a las precondiciones, si los terminales tienen como requisito el soporte de estas (precondiciones deseadas, precondiciones satisfechas actualmente, precondiciones que se tienen que cumplir, etc.)

El siguiente ejemplo muestra como se incorpora el paquete SDP dentro del mensaje inicial SIP INVITE de solicitud de sesión enviada por un usuario a la red:

```
INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Supported: 100rel
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-
c=8642; port-s=7531
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE

Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99          // medio solicitado
b=AS:75                              //ancho de banda para el medio
a=curr: qos local none               //precondiciones del usuario
a=des:qos mandatory local sendrecv   //precondiciones a cumplir usuario
a=curr:qos remote none               //estado actual de las precondiciones
a=des:qos none remote sendrecv       //precondiciones en el usuario remoto
a=rtpmap:98 H263                     //códec 1 para el medio solicitado
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES                  //códec 2 para el medio solicitado
```

Si un terminal de destino no soportase un medio en concreto, en la respuesta enviada a la solicitud del otro usuario indicaría que el puerto para ese medio es 0. Si un terminal no soporta alguno de los códec propuestos por el otro usuario no incluye en la descripción de dicho medio una línea para ese formato o códec.

5.5.7. Reserva de recursos

Una vez que los terminales de usuario se han puesto de acuerdo en la negociación de medios, el siguiente paso es la reserva de los recursos necesarios en las redes de acceso y en la red troncal de cada usuario que permita la comunicación entre usuarios en los términos acordados.

Durante la negociación de los medios, los P-CSCF de cada usuario extraen los paquetes SDP contenidos en la señalización SIP y envían la

información relevante de la sesión a la función de control de política de red y tarificación (PCRF) que en base a la información obtenida calcula la autorización a los recursos necesarios para cumplir con la QoS determinada. Esta autorización estará expresada en términos de qué recursos IP pueden ser accedidos por el usuario en el nivel de recursos de la red multimedia (MRF).

Cuando la solicitud de reserva de recursos llega a la pasarela de la red de acceso, esta comprueba que los parámetros solicitados están dentro de los parámetros autorizados por el PCRF, si es así, el PCEF en la red de acceso inicia el establecimiento de una portadora de medios que satisfaga la petición (o modifica una existente si ya estuviera establecida) para la red de acceso (En el caso de GPRS esto se traduce en el establecimiento o modificación de un contexto PDP para los medios) y para la red troncal (recursos IP requeridos en el MRF). Una vez que se han reservados con éxito los recursos solicitados en uno de los extremos, se confirma a través de un mensaje de señalización SIP UPDATE que las precondiciones impuestas se han cumplido en ese extremo. Cuando las precondiciones también se cumplen por parte del otro extremo, se envía la correspondiente confirmación en un mensaje de respuesta SIP 200 OK.

```
UPDATE <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:orig@scscf1.home1.net;lr>
From: <sip:user1_public1@home1.net>; tag=171828
To: <tel:+12125552222> tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 129 UPDATE
Require: sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; ealg=aes-cbc; spi-c=98765432; spi-
s=87654321; port-c=8642; port-s=7531
Contact: <sip:user1_public1@home1.net;gr=urn:uuid:f81d4fae-7dec-11d0-a765-
00a0c91e6bf6;comp=sigcomp>
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local sendrececv     //reserva de recursos en el usuario llamante
                                //confirmada
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
```

El diagrama completo es el que muestra la ilustración siguiente donde se pueden observar los procesos de autorización de recursos durante la negociación de medios y la posterior reserva de los mismos una vez que recursos han sido acordados.

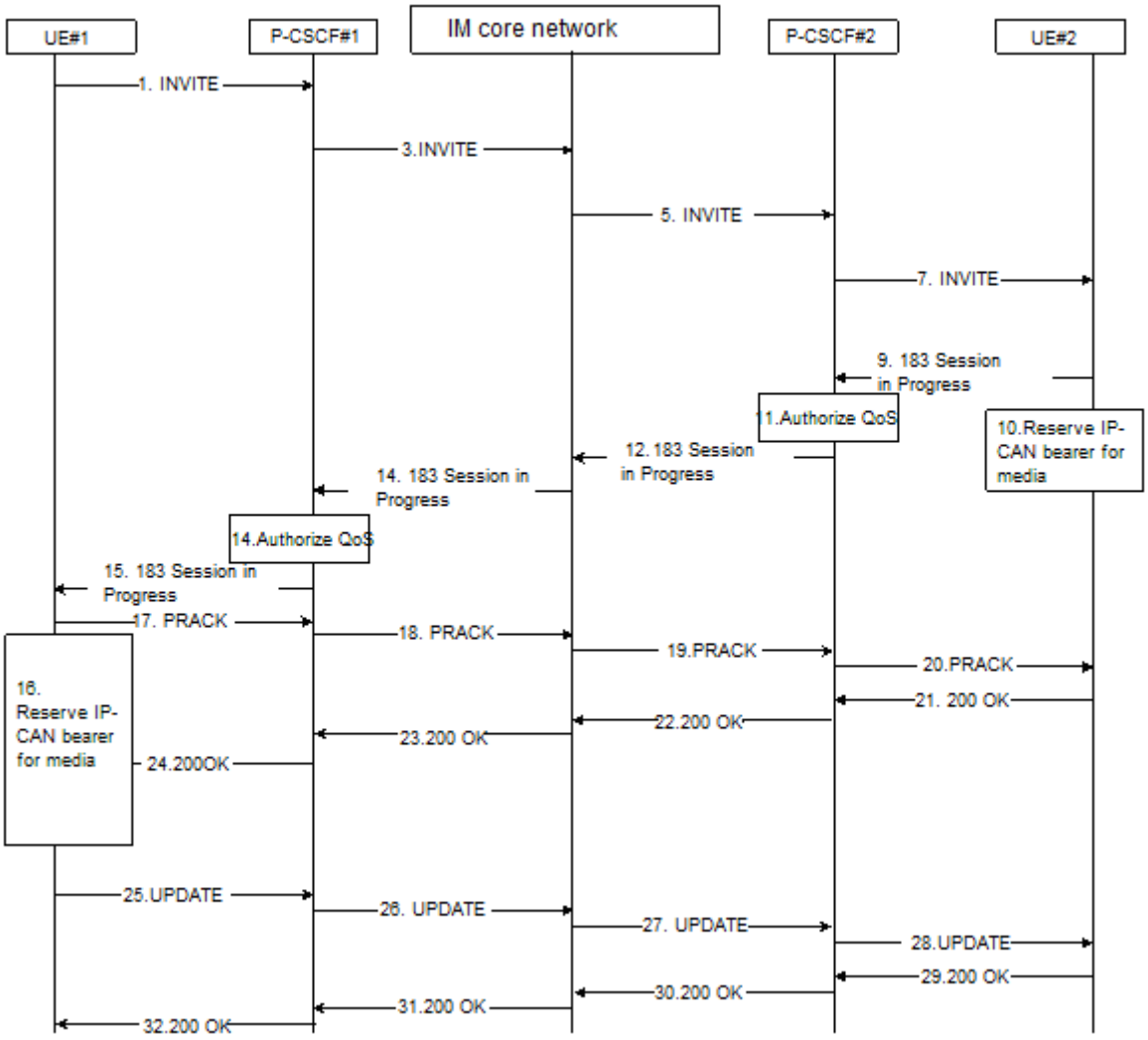

Figura 57. Autorización y reserva de recursos.

5.6. Flujos de inicio de sesión multimedia

5.6.1. Introducción

Para el establecimiento de una sesión IP multimedia extremo a extremo se tienen que darse lo siguientes pasos:

- Flujo de señalización de origen, entre el usuario que origina la sesión y la red.
- Flujos entre entidades de la misma red troncal o entre entidades de redes distintas.
- Flujo de señalización de terminación, entre la red y el destinatario de la sesión.

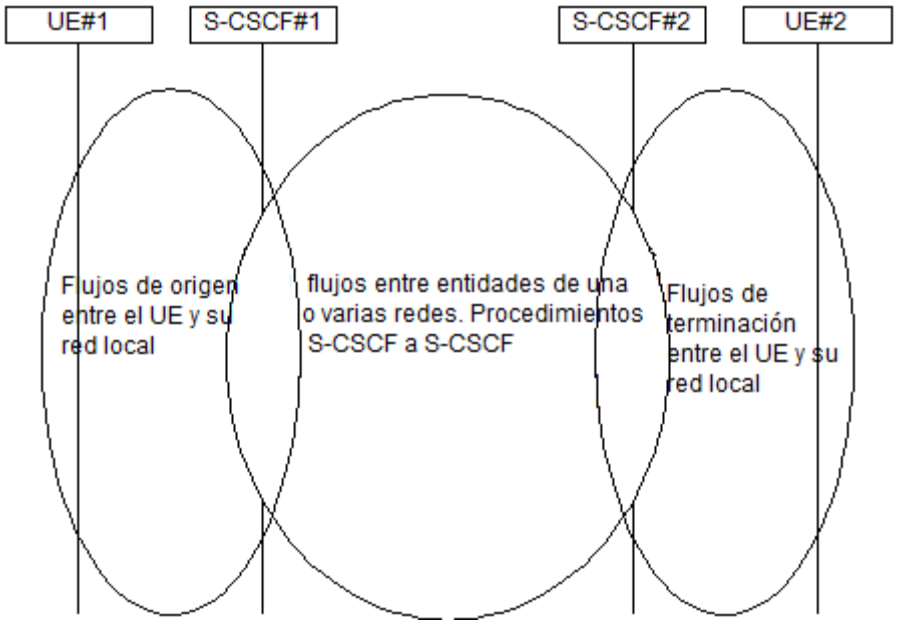

Figura 58. Flujos de señalización en una sesión multimedia.

5.6.2. Flujos de origen de sesión

Es el intercambio de mensajes de señalización que tiene lugar entre el usuario que solicita el establecimiento de una sesión multimedia con la entidad de control del usuario que gestionará y controlará la sesión solicitada (S-CSCF). En este tipo de flujos diferenciaremos aquellos que son iniciados dentro de la red multimedia (IMS) y lo que se originan en la red pública conmutada (PSTN) o en una red IP distinta de la red multimedia (red conmutada de paquetes) puesto que tendrán un tratamiento distinto en cada caso.

5.6.2.1. Sesión iniciada por un terminal registrado en la red multimedia (IMS)

Este caso tiene lugar cuando el terminal del usuario en cuestión, está registrado a través de la red de acceso IP utilizada (IP-CAN) directamente con la red multimedia. Existen dos casos, cuando el usuario está localizado en la red local (Home Network) y cuando lo está en una red de tránsito o roaming (Visited Network). La diferencia desde el punto de vista de los mensajes intercambiados en mínima puesto que solo afecta en donde estará ubicado el P-CSCF con el que se comunica el usuario, o bien en la red local del usuario o bien en la red visitada donde se encuentre temporalmente ubicado el usuario. El siguiente diagrama muestra todos los mensajes intercambiados que explicaremos a continuación. No entraremos en la descripción formal de los mensajes para tratar de centrarnos en la funcionalidad de los mismos:.

Mensajes 1 y 3: El usuario que desea iniciar la sesión multimedia, una vez que se encuentra registrado y ha establecido las asociaciones de seguridad e integridad requeridas por la red, construye la petición de inicio de sesión SIP INVITE. Este primer mensaje incorpora información de quien quiere iniciar la sesión (dirección IP del terminal), como enrutar el mensaje (como llegar hasta la entidad de control S-CSCF) e información de descripción de sesión SDP en el cuerpo del mensaje para la negociación de las características de la sesión. También incluirá información de compresión de los mensajes en la comunicación con el P-CSCF.

Mensajes 2 y 4: Respuesta provisionales de recepción y tramitación de la petición de sesión.

Mensajes 5 y 6: Una vez que la petición llega al S-CSCF que controla al usuario, comprueba si el usuario tiene permisos para acceder al servicio solicitado (Consultando el perfil de usuario descargado del HSS durante el proceso de registro) y determina en función de la URI recibida en el paquete (identidad publica del usuario de destino) cual será la siguiente entidad a la que retransmitir el mensaje.

Mensajes 8 9 y 11: Una vez que el mensaje llegue al destinatario y este genere una respuesta, ésta se transmite por el mismo camino hacia el origen. Este mensaje incluye una respuesta SDP a la oferta inicial realizada por el usuario de origen incluyendo los parámetros soportados por el destinatario.

Mensaje 10: Cuando la respuesta SDP llega al P-CSCF este solicita una autorización para los recursos de esta sesión al control de recursos de la red (PCRF). Esta entidad determinará qué recursos estarán permitidos en la sesión.

Mensajes 12, 14 y 15: El terminal de usuario de origen, recibe la respuesta SDP del destinatario y selecciona el subconjunto de características que soporta este último y que cumplen con las preferencias del usuario inicial y envía un mensaje PRACK para indicar los parámetros SDP elegidos y recibir confirmación del destinatario. Si no hubiera coincidencia, entonces el terminal del usuario inicial generaría una solicitud con nuevos parámetros.

Mensajes 16,17 y 18: Se recibe la segunda respuesta SDP a la selección de parámetros realizada por el terminal de origen con la confirmación del destinatario. Si no había coincidencia en el punto anterior entonces continúa la negociación hasta que se alcanza.

Mensaje 13: Al recibir la confirmación del destinatario, el terminal de usuario inicia la reserva de recursos. Envía una petición a la red de acceso con los recursos requeridos y la función PCEF la ejecuta dentro de los parámetros permitidos por la autorización dada en el mensaje 10 por el PCRF.

Mensajes 19, 20, 21: Cuando los recursos están reservados, se envía una confirmación de que los recursos ya están listos para usarse. En este mensaje se indica que el usuario inicial ya cumple las precondiciones impuestas.

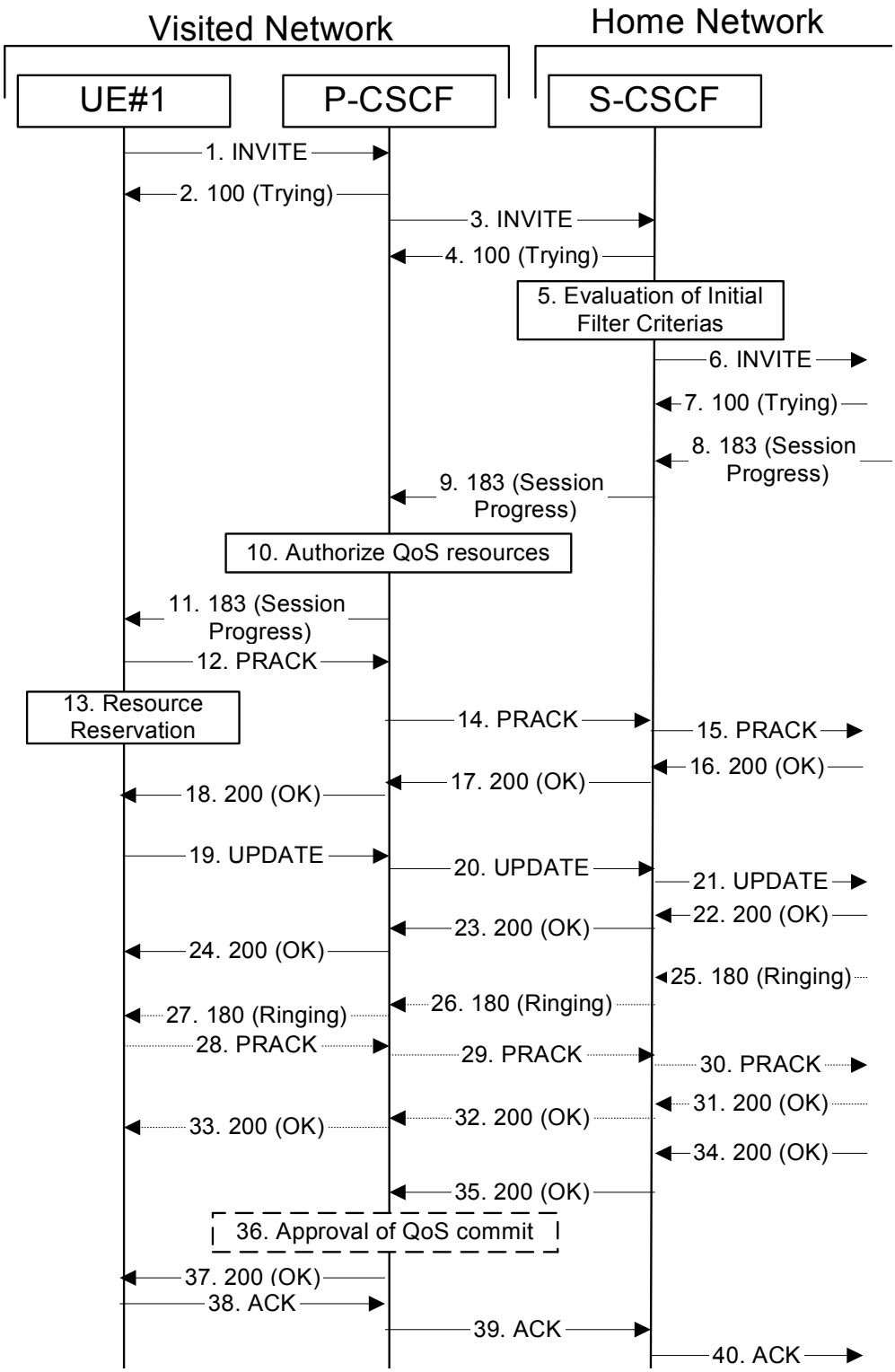

Figura 59. Flujo de señalización iniciada en la red IMS

Mensajes 22, 23, 24: Cuando los recursos estén reservados en el destinatario se envía confirmación hacia el origen del cumplimiento de las precondiciones.

Mensajes: 25, 26, 27: Después de cumplirse las precondiciones, la red de destino inicia la alerta al terminal del usuario del destinatario y lo indica con un mensaje de "ring back" hacia el origen.

Mensajes 28, 29 y 30: El origen envía acuse de recibo del mensaje de alerta al destinatario.

Mensajes 31, 32 y 33: respuesta al acuse de recibo anterior.

Mensajes: 34, 35 y 37: Cuando el destinatario responde a la llamada, la red de destino envía un mensaje de respuesta final a la solicitud de inicio de sesión INVITE del mensaje 1.

Mensaje 36: El P-CSCF de origen al recibir la respuesta final de inicio de sesión, habilita el acceso del terminal de usuario de origen a los recursos reservados previamente.

Mensajes 38, 39 y 40: confirmación del terminal de usuario a la recepción de la respuesta final del destinatario.

La figura 58 muestra el flujo de mensajes de de inicio de sesión

5.6.2.2. Sesión o llamada originada en el dominio de circuitos conmutados (PSTN)

Cuando el origen de la sesión no es un terminal registrado en la red multimedia, sino que es un terminal registrado que pertenece al dominio de circuitos conmutados, este procedimiento ilustra cómo se inicia la solicitud de sesión a la entrada en la red multimedia. El punto de entrada en este caso es el MGCF, que será la función encargada de hacer de pasarela entre el dominio de circuitos y la red multimedia. El diagrama de la figura 45 ilustra como el MGCF convierte la señalización de la red de circuitos a la señalización SIP y como controla la pasarela de medios para adaptar los formatos de los medios que se establecerán en la sesión.

Mensaje 1: El MGCF recibe un mensaje de señalización IAM (señalización SS7) de la red de circuitos conmutados para iniciar una sesión en la red multimedia.

Mensaje 2: El MGCF inicia la comunicación hacia el MGW para establecer una conexión entre dominios.

Mensaje 3: El MGCF construye una petición SIP INVITE a partir de la información recibida en el mensaje recibido del dominio de circuitos , dirigido al

Tel URI o al SIP URI del destinatario, incluyendo un primer mensaje SDP con la descripción de medios y características soportadas por el terminal 1.

Mensaje 5: La respuesta SDP llega al MGCF con las capacidades del destinatario.

Mensaje 6: El MGW inicia la negociación de portadora con el dominio de circuitos si fuera necesario.

Mensajes 7 y 8: Se selecciona y confirma el conjunto de parámetros elegidos por el origen o si fuera necesario se continúa negociando los parámetros de la sesión con una segunda oferta/respuesta en la confirmación a la respuesta de la primera oferta y su correspondiente respuesta.

Mensaje 9 y 10: El MGCF da instrucciones al MGW para que inicie la reserva de recursos acordados.

Mensajes 12 y 13: Cuando los recursos están reservados se comunica hacia los dos extremos.

Mensaje 14 y 15: Cuando las precondiciones se cumplen en ambos extremos la red de destino alerta al terminal del destinatario e informa al MGCF y este responde al mensaje.

Mensaje 17: Cuando el destinatario está siendo alertado el MGCF informa al dominio de circuitos con un mensaje ACM (señalización SS7) para que informe al usuario que origina la sesión.

Mensaje 18: El MGCF recibe la respuesta final del destinatario 200 OK.

Mensaje 19: El MGCF informa al dominio de circuitos de la respuesta final del destinatario con el mensaje ANM (señalización SS7)

Mensaje 20: El MGCF instruye al MGW para la activación de la conexión entre dominios.

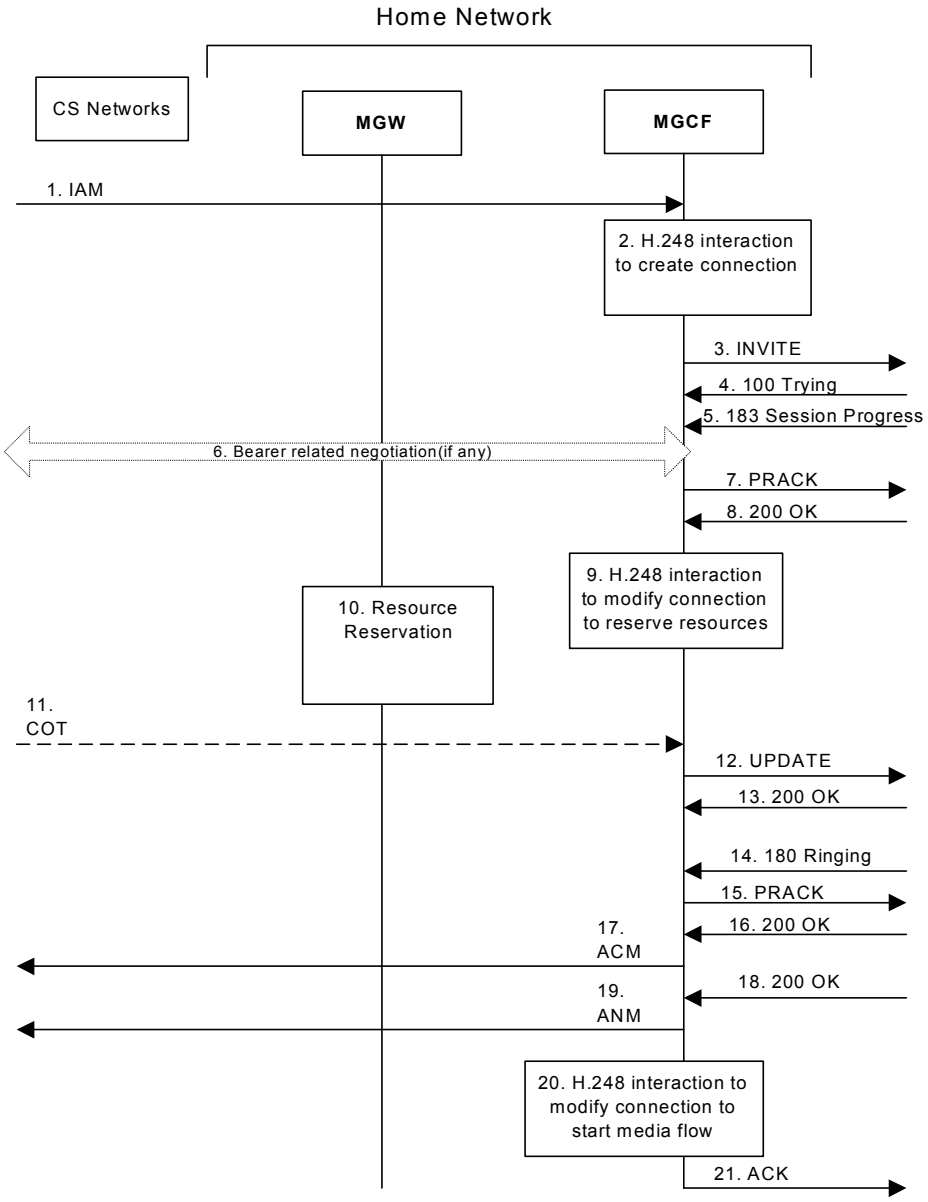

Figura 60. Flujo de señalización entre PSTN-MGCF

5.6.2.3. Sesión originada en una red IP externa (No IMS)

Cuando la sesión se origina en un usuario SIP externo que no pertenece a la red multimedia pueden darse varias situaciones, si el cliente SIP externo soporta las extensiones de SIP usadas en la red multimedia, su comportamiento no varía del caso explicado en el punto 5.6.2.1.

Si por el contrario el cliente SIP del usuario de la red externa no soporta la imposición de precondiciones (extensión SIP si soportadas en la red multimedia) entonces la sesión la red multimedia asume que el endpoint de origen externo ya tiene reservado y disponible los recursos incluidos en el INVITE inicial (por ejemplo el caso de un cliente SIP en un dispositivo conectado por cable a una red ADSL). En esta situación el terminal de origen

indicará en la descripción del mensaje SDP inicial los medios disponibles y las características que utilizará en
cada uno de los mismos sin establecer una negociación con el terminal de destino (sin precondiciones) e indicando que ya están disponibles (media set = "active") mientras que el terminal de terminación sí que realizará el proceso de reserva de recursos en la red multimedia ajustándose a la información de medios proporcionada en la petición de sesión. Si el terminal de usuario o la red multimedia no soportasen algunas de las características o de los medios indicados por el origen el establecimiento de llamada será rechazado con un mensaje SIP 420 Bad Request. Durante el proceso de reserva de recursos en la terminación los medios no estarán accesibles (media set= "inactive") para ambos terminales hasta que el usuario de destino responda. Cuando el usuario responde y envía el mensaje aceptación de la sesión (200 OK) se activa el acceso a los medios para ambos terminales de usuario y el establecimiento de la sesión. La figura siguiente ilustra el proceso descrito.

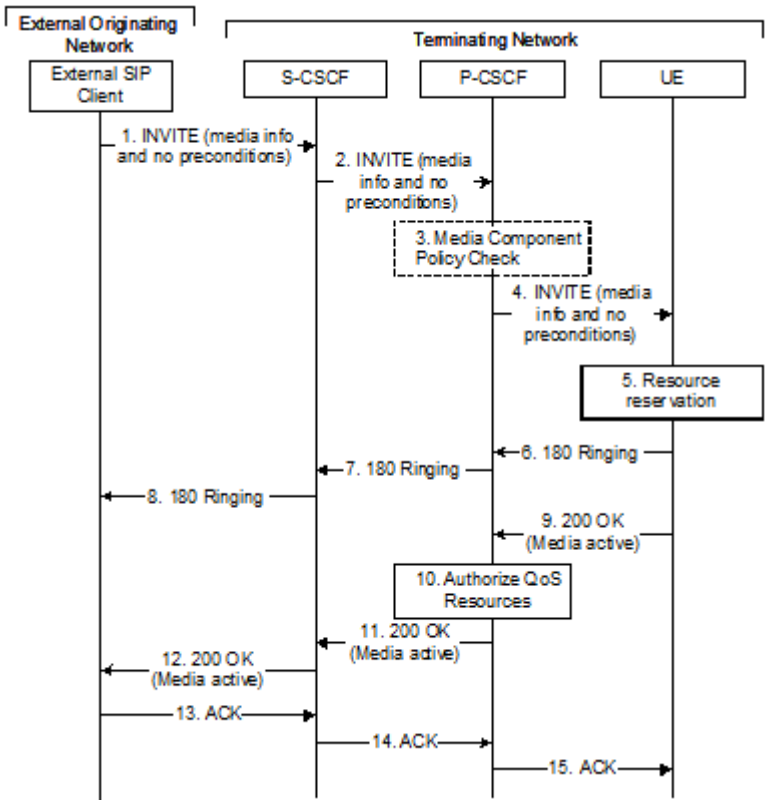

Figura 61. Diagrama de sesión de cliente SIP externo de origen sin soporte de precondiciones.

5.6.3. Flujos de señalización de sesión en la red troncal.

Es el intercambio de mensajes de señalización que tiene lugar entre el S-CSCF/MGCF que controla al usuario que origina la sesión y el S-CSCF/ MGCF que controla al usuario de terminación. Existen diferentes posibilidades, que el

tanto el origen como la terminación de la sesión se producen en la misma red, el origen y la terminación de la sesión se realizan en redes diferentes, la terminación se produce en el dominio PSTN desde la propia red multimedia o la terminación se produce en el dominio PSTN a través de una red multimedia de tránsito.

5.6.3.1. Origen y terminación de la sesión en la misma red multimedia

Cuando el S-CSCF recibe la petición del usuario que origina la sesión, analiza la dirección de destino y determina que pertenece a un suscriptor del mismo operador de red. En ese momento se determinará que S-CSCF está en servicio para ese destinatario, preguntando al HSS a través del I-CSCF cuál es el S-CSCF que sirve en esos momentos al destinatario. Describimos algunos de los mensajes intercambiados en la red multimedia del siguiente flujo.

Mensaje 4: El S-CSCF/MGCF del usuario de origen (S-CSCF#1 en la figura) envía el mensaje de inicio de sesión (INVITE) con la primera oferta SDP al I-CSCF.

Mensaje 6: El I-CSCF pregunta al HSS de la red cual es el S-CSCF que controla al usuario de destino (S-CSCF#2)

Mensaje 7: El I-CSCF retransmite el mensaje de inicio de sesión (INVITE) al elemento de control del destinatario (S-CSCF#2)

Mensajes 12, 13, 14 y 15: La respuesta a la oferta SDP enviada en el mensaje INVITE atraviesa el camino de señalización por la red troncal establecido en los pasos anteriores hacia el usuario de origen.

Mensajes 16, 17, 18: El origen decide el conjunto de parámetros de la sesión y se los indica al destinatario a través del mensaje PRACK. A partir de este instante los siguientes mensajes de solicitud y de repuesta a los mismos que tengan lugar dentro del dialogo actual, no atravesarán la entidad I-CSCF, sino que se retransmitirán directamente entre un S-CSCF y el otro, puesto que ya conocen la dirección de la entidad que controla al usuario contrario.

Mensajes 19, 20, 21: El destinatario responde a la oferta incluida en el mensaje anterior.

Mensajes 22, 23, 24: Confirmación de recursos disponibles por el usuario de origen.

Mensajes 25, 26, 27: Confirmación de recursos disponibles por el destinatario.

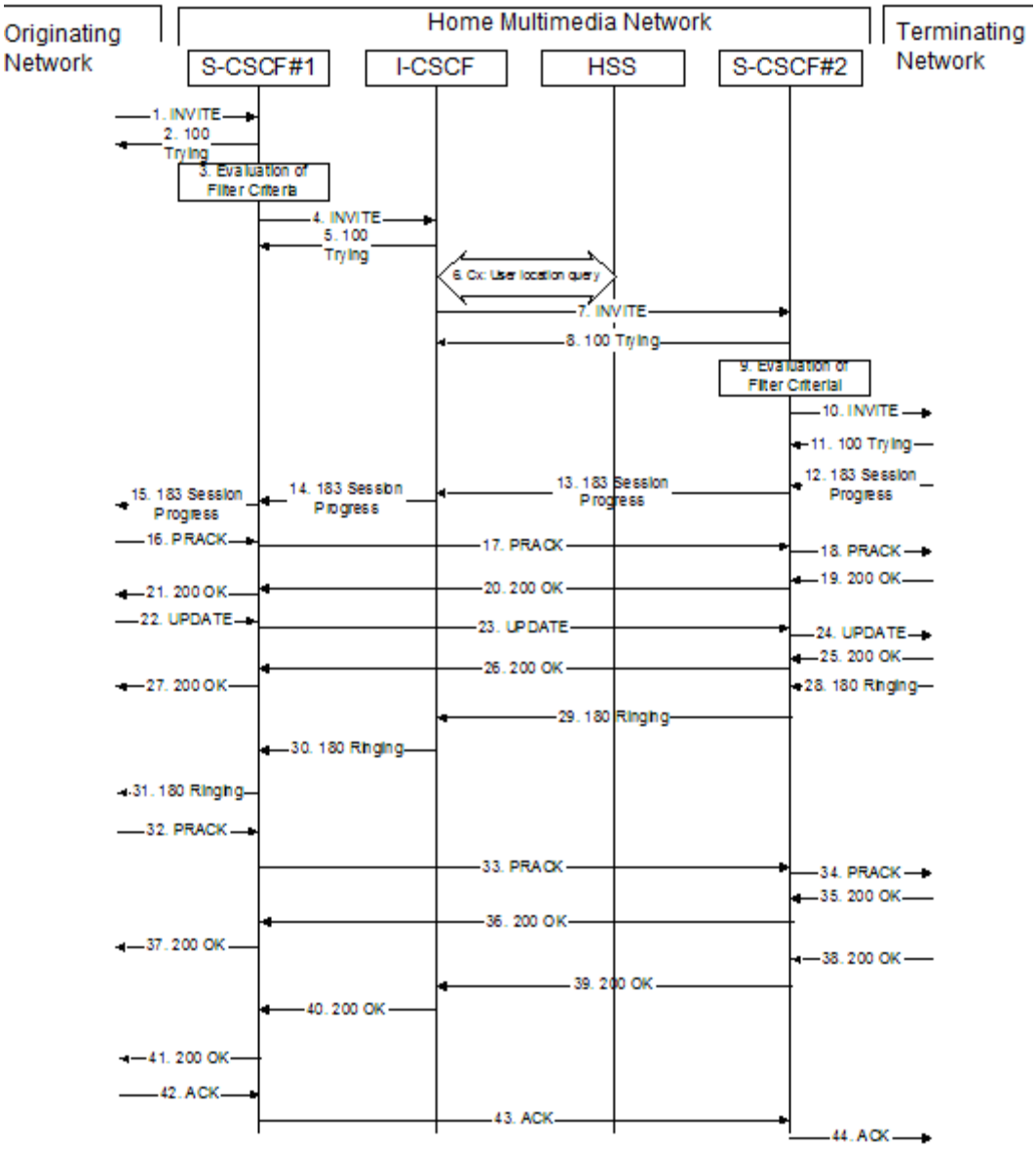

Figura 62. Diagrama de sesión iniciada y terminada en la misma red multimedia

Mensajes 28, 29, 30, 31: Información hacia el origen de que el destinatario está siendo alertado de la llamada.

Mensajes 32-37: mensaje de acuse de recibo de la información de alerta de destinatario y su correspondiente respuesta.

Mensajes 38, 39, 40, 41: Respuesta final a la petición de sesión inicial por el destinatario.

5.6.3.2. Origen y terminación en redes multimedia diferentes

Cuando el S-CSCF recibe la petición del usuario que origina la sesión, analiza la dirección de destino y determina que pertenece a un suscriptor de un operador de una red multimedia diferente. En ese momento reenvía al punto de entrada en la red de destino (I-CSCF) el mensaje de solicitud de sesión. En este punto seguirá con el mismo procedimiento que el caso 5.6.3.1, preguntará al HSS cuál es el S-CSCF que sirve en esos momentos al destinatario en la red de destino. Describiremos algunos de los mensajes intercambiados en la red multimedia que se muestran en el siguiente flujo.

Puede darse una variante y es que en lugar de comunicarse a través de la función I-CSCF es posible que los distintos dominios los hagan a través de las funciones IBCF. La introducción de estas entidades tiene sentido cuando los operadores de red requieren funciones de encapsulamiento de topología de red (THIG), destinada a ocultar parcial o totalmente información sensible de la arquitectura de la red a otros operadores.

El flujograma de mensajes de señalización es análogo al descrito en el apartado 5.6.3.1 con la salvedad de que la función I-CSCF (o IBCF si se requiriera encapsulamiento de la arquitectura de la red) se encuentra localizada en la red de destino.

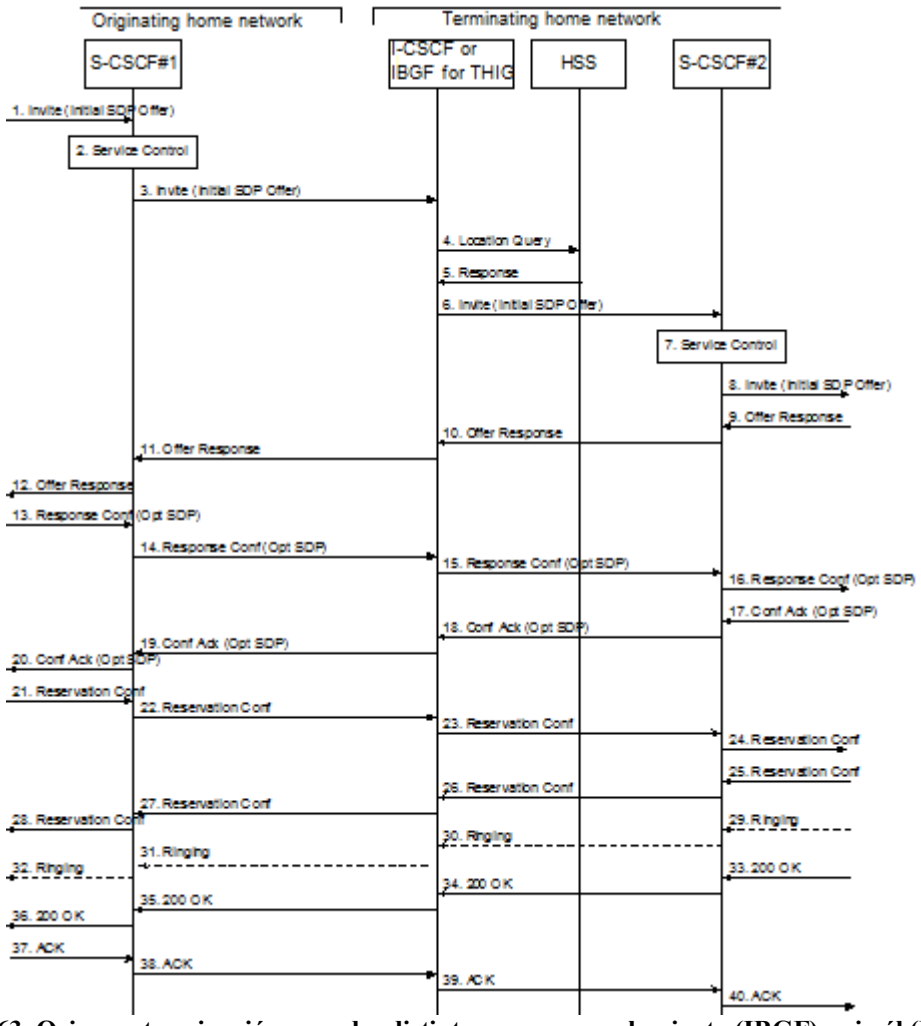

Figura 63. Origen y terminación en redes distintas con encapsulamiento (IBGF) o sin él (I-CSCF)

5.6.3.3. Terminación de sesión en la red pública conmutada (PSTN) a través de la propia red multimedia.

El S-CSCF que gestiona al usuario inicial analiza la dirección del destinatario y determina que se trata de un usuario de la red pública conmutada. Entonces el S-CSCF reenvía la petición a un BGCF local, éste realiza análisis adicionales de la dirección del destinatario y determina que la terminación hacia la red de circuitos se realiza a través de la propia red multimedia. A continuación el BGCF selecciona un MGCF en la red multimedia para que éste realice el proceso de interconexión con la red de circuitos interconectada. El siguiente diagrama muestra el flujo de información descrito y donde se describe la señalización más relevante:

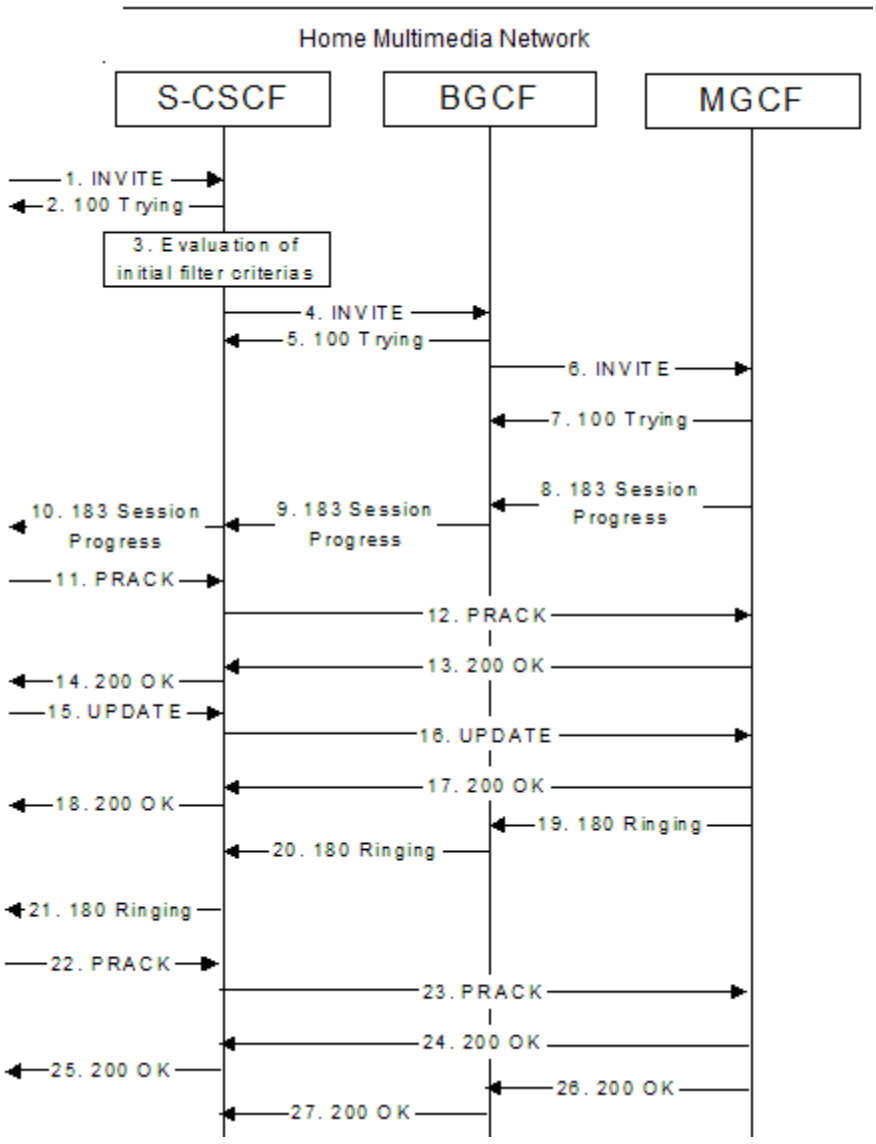

Figura 64. Terminación en la red PSTN desde la misma red local del usuario que inicia la sesión.

Mensaje 1: Mensaje de inicio de sesión recibido del usuario que solicita la sesión. Este puede seguir cualquier cualquiera de los esquemas de

origen descritos, Si la solicitud de sesión viniera de un usuario de la red PSTN, el S-CSCF se sustituiría por el MGCF#1 que controlaría al usuario inicial.

Mensaje 3 y 4: El S-CSCF (o MGCF en su defecto) determina que el destinatario es un usuario de la red pública conmutada en base a la dirección de destino y remite la petición al BGCF de la red multimedia.

Mensaje 6: El BGCF determina, en base a la dirección y los acuerdos establecidos con otros operadores, que para ese usuario la terminación hacia la red de conmutación de circuitos se realizará en la propia red multimedia. Selecciona el MGCF que controlará las funciones de conversión (señalización y medios) hacia la red PSTN del destinatario y le envía la petición de sesión.

Mensajes 8, 9, y 10: El MGCF recibe la respuesta a la oferta de medios incluida en la petición inicial enviada a la red pública conmutada y la retransmite hacia el origen de la sesión siguiendo a la inversa el camino recorrido por el mensaje INVITE.

Mensajes 11, 12: El origen responde con la confirmación de los medios elegidos al destinatario si hubiera que realizar tan acción o con una segunda oferta si todavía no hubiera acuerdo de medios. En principio el BGCF puede permanecer o no en el camino de señalización para las peticiones generadas posteriormente dentro del dialogo de sesión. Si no lo hace la comunicación se hace entre el S-CSCF del usuario inicial y el MGCF que controla la interconexión con el destinatario.

El resto de mensajes son exactamente iguales que en los casos descritos en los puntos 5.6.3.1 y 5.6.3.2.

5.6.3.4. Terminación de sesión en la red pública conmutada PSTN a través de una red multimedia de transito.

El S-CSCF que gestiona al usuario inicial analiza la dirección del destinatario y determina que se trata de un usuario de la red pública conmutada. El S-CSCF reenvía la petición a un BGCF local y éste realiza análisis correspondientes de determinar cuál es la pasarela más apropiada hacia ese dominio. En este caso establece que la terminación hacia la red de circuitos se realiza a través de una red multimedia de tránsito de otro operador. A continuación el BGCF de la red local (BGCF#1) selecciona un BGCF en la red multimedia de tránsito (BGCF#2) y éste a su vez asignará un MGCF dentro de la red de tránsito para que gestione la interconexión con la red de circuitos conmutados final. El siguiente diagrama muestra el flujo de información descrito y los mensajes más relevantes:

Mensaje 1: Mensaje de inicio de sesión recibido del usuario que solicita la sesión. Este puede seguir cualquier cualquiera de los esquemas de origen descritos, Si la solicitud de sesión viniera de un usuario de la red PSTN, el S-CSCF se sustituiría por el MGCF#1 que controlaría al usuario inicial.

Mensaje 3: El S-CSCF (o MGCF en su defecto) determina que el destinatario es un usuario de la red pública conmutada en base a la dirección de destino.

Mensaje 4: El S-CSCF selecciona el BGCF que determinará donde se produce la terminación y le reenvía la petición de sesión.

Mensaje 6: El BGCF de la red local del origen, a partir de la dirección del destinatario y de los acuerdos de interconexión con otros operadores, selecciona cual será el operador de red que mejor terminará esa sesión. El BGCF#1 selecciona el BGCF#2 en la red del operador de tránsito.

Mensaje 8: El BGCF#2 de la red destino selecciona el MGCF que controlará las funciones de conversión (de señalización y de medios) hacia la red PSTN final y le envía la solicitud de sesión.

Mensajes 10, 11, 12 y 13: El MGCF recibe la respuesta a la oferta de medios incluida en la petición de sesión enviada a la red pública conmutada de destino y la retransmite hacia el origen de la sesión.

Mensajes 14 y 15: El origen responde con la confirmación de los medios elegidos al destinatario si tuviera que realizar tan acción o con una segunda oferta si no hubiera acuerdo de medios aún. Los BGCFs de ambas redes pueden permanecer o no en el camino de señalización para las peticiones generadas posteriormente dentro del dialogo de sesión. Si no es así, la comunicación se hace directamente entre el S-CSCF del usuario inicial y el MGCF que controla la interconexión con el destinatario.

El resto de mensajes son exactamente iguales que en los casos descritos en los puntos 5.6.3.1 y 5.6.3.2, por lo que no volveremos sobre ellos.

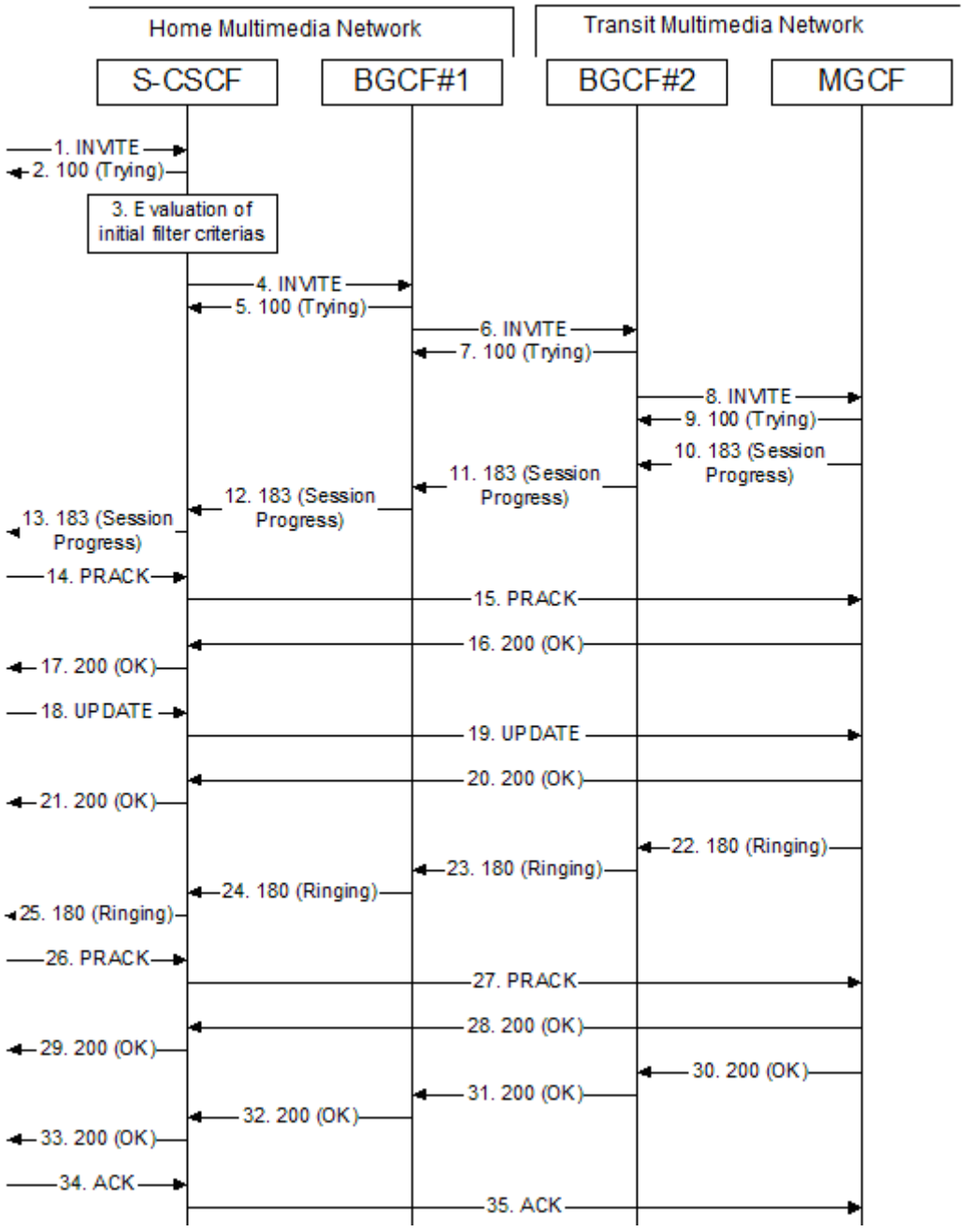

Figura 65. Terminación en la red PSTN desde una red diferente a la del usuario que inicia la sesión.

5.6.4. Flujos de terminación de sesión

Es el intercambio de mensajes que se produce entre la entidad de control del destinatario final (S-CSCF#2) y el terminal del destinatario para hacer llegar una petición de sesión multimedia iniciada por otro usuario. El camino de señalización entre el terminal y el control de la red como se ha comentado anteriormente es conocido por ambos y se estableció durante el proceso de registro del terminal de destino en la red local de destino del usuario final.

Como en el caso de flujos de inicio de sesión del punto 5.6.2, en función del tipo de la localización del terminal pueden darse diferentes casos, si la terminación tiene lugar en el dominio multimedia (terminación IMS), si la terminación tiene lugar en la red conmutadas de circuitos (PSTN) entonces el procedimiento será la continuación del descrito en los puntos 5.6.3.3 y 5.6.3.4, o si la terminación se produce en una red de IP distinta.

5.6.4.1. Destinatario registrado en la red multimedia (IMS)

Este caso tiene lugar cuando el terminal del destinatario está registrado a través de una red de acceso IP (IP-CAN) en la red multimedia. Existen dos casos, cuando el usuario está localizado en la red local (Home Network) y cuando lo está en una red de transito o roaming (Visited Network). La diferencia desde el punto de vista de los mensajes intercambiados es pequeña puesto que esto sólo afecta en donde estará ubicado el P-CSCF con el que se comunica el destinatario, en su red local o en una red visitada. El siguiente diagrama muestra todos los mensajes intercambiados para el caso de que el usuario final se encuentre en roaming, si se encontrase conectado directamente a la red local los mensajes intercambiados serían los mismos.

Este procedimiento es el equivalente del explicado en el punto 5.6.2.1 pero para el usuario que recibe la petición de sesión.

Mensajes 1 y 3: El control del destinatario recibe una petición de inicio de sesión SIP INVITE y determina si el usuario tiene permisos para acceder al servicio solicitado (Consulta al perfil del destinatario descargado del HSS durante el proceso de registro) y determina en función de la URI recibida en el paquete (identidad publica del usuario de destino) cual será la siguiente entidad a la que retransmitir el mensaje.

Mensaje 4 y 6: Envía la petición a través del camino de señalización establecido durante el registro del destinatario.

Mensajes 8, 10 y 11: Una vez que el mensaje llegue al destinatario y este genere una respuesta esta se transmite por el mismo camino hacia el origen. Este mensaje incluye una respuesta SDP a la oferta inicial por el usuario de origen con los parámetros soportados por el destinatario.

Mensaje 9: Cuando la respuesta SDP llega al P-CSCF que conecta con el destinatario este solicita una autorización de acceso a los recursos al control de recursos de la red (PCRF).

Mensajes 12, 13 y 14: El terminal de usuario de origen, recibe la respuesta SDP del destinatario y selecciona el subconjunto de características que soporta este último y que cumplen con las preferencias del usuario inicial y envía un mensaje PRACK para indicar los parámetros SDP elegidos y recibir confirmación del destinatario . Si no hubiera coincidencia, entonces el terminal del usuario inicial generaría una nueva solicitud con nuevas características.

Mensajes 15, 16 y 17: Se envía la segunda respuesta SDP a la segunda oferta con la confirmación del destinatario de los medios a utilizar. Si no hubiera coincidencia en el punto anterior entonces continúa la negociación hasta que se ésta se alcanza.

Mensaje 18: El terminal del destinatario al enviar confirmación de los medios a utilizar, inmediatamente inicia la reserva de recursos. Envía una petición a la IP-CAN con los recursos requeridos y la función PCEF la ejecuta dentro de los parámetros permitidos por la autorización dada en el mensaje 9 por el PCRF.

Mensajes 19, 20, 21: Cuando los recursos están reservados, se envía una confirmación de que los recursos ya están listos para usarse. En este mensaje se indica que el usuario inicial ya cumple las precondiciones impuestas.

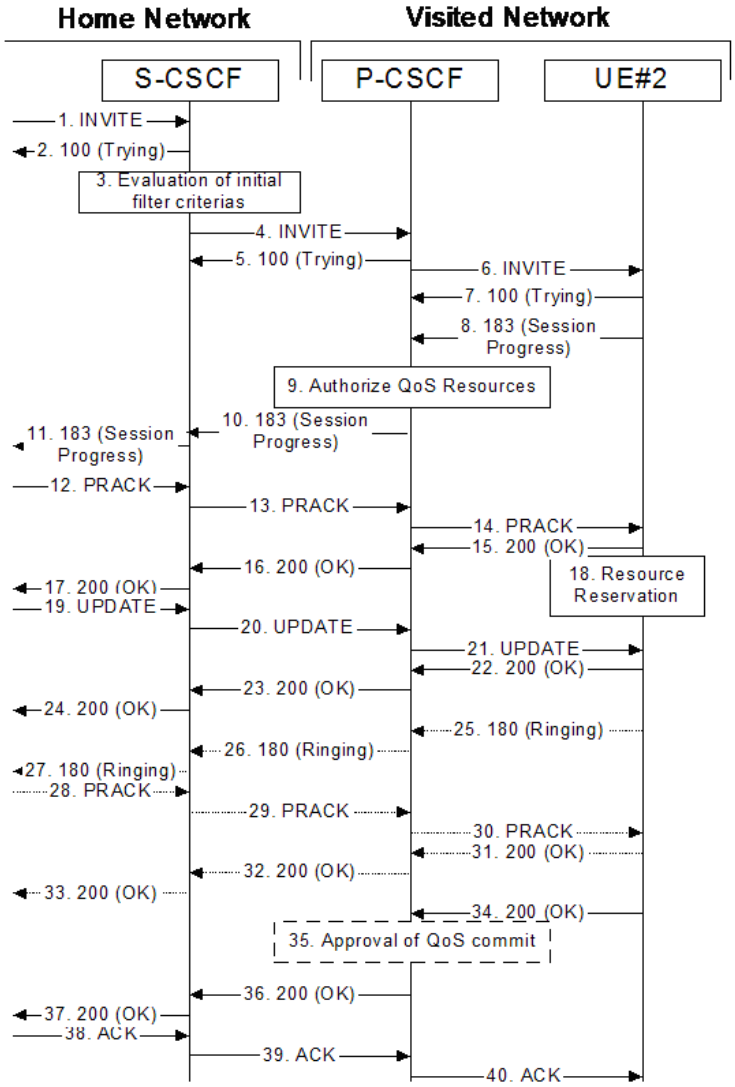

Figura 66. Procedimiento de terminación de sesión cuando el destinatario pertenece a la red IMS

Mensajes 22, 23, 24: Cuando los recursos estén reservados en el destinatario se envía confirmación hacia el origen del cumplimiento de las precondiciones.

Mensajes: 25, 26, 27: Después de cumplirse las precondiciones, la red de destino inicia la alerta al terminal del usuario del destinatario y lo indica con estos mensajes hacia el origen.

Mensajes 28, 29 y 30: El origen envía acuse de recibo del mensaje de alerta al destinatario.

Mensajes 31, 32 y 33: respuesta al acuse de recibo anterior.

Mensajes: 34, 36 y 37: Cuando el destinatario responde a la llamada, la red de destino envía un mensaje de respuesta final a la solicitud de inicio de sesión INVITE del mensaje 1.

Mensaje 35: El P-CSCF al recibir la respuesta final de inicio de sesión, permite el acceso del terminal de usuario a los recursos reservados previamente.

Mensajes 38, 39 y 40: confirmación del terminal de usuario a la recepción de la respuesta final del destinatario.

5.6.4.2. Sesión o llamada con destinatario en el dominio de circuitos conmutados (PSTN)

Cuando el destino de la sesión no es un terminal registrado en la red multimedia, sino que es un terminal que pertenece al dominio de circuitos conmutados, este procedimiento ilustra cómo se termina la solicitud de sesión a la salida de la red multimedia. El punto de salida en este caso es el MGCF, que será la función encargada de realizar la interconexión entre el dominio de circuitos y la red multimedia. El diagrama de la figura siguiente muestra como el MGCF convierte la señalización SIP a señalización SS7 y como instruye a la pasarela de medios para ajustar los formatos de los medios entre uno y otro dominio.

Mensaje 1: El MGCF recibe un mensaje de señalización de inicio de sesión SIP INVITE con su correspondiente oferta de medios realizada por el origen.

Mensaje 3: El MGCF interactúa con el MGW para establecer un canal de salida hacia el dominio de circuitos y determina las capacidades de los medios de la pasarela.

Mensaje 4: El MGCF construye un mensaje de señalización IAM (SS7) a partir de la información recibida en la petición SIP.

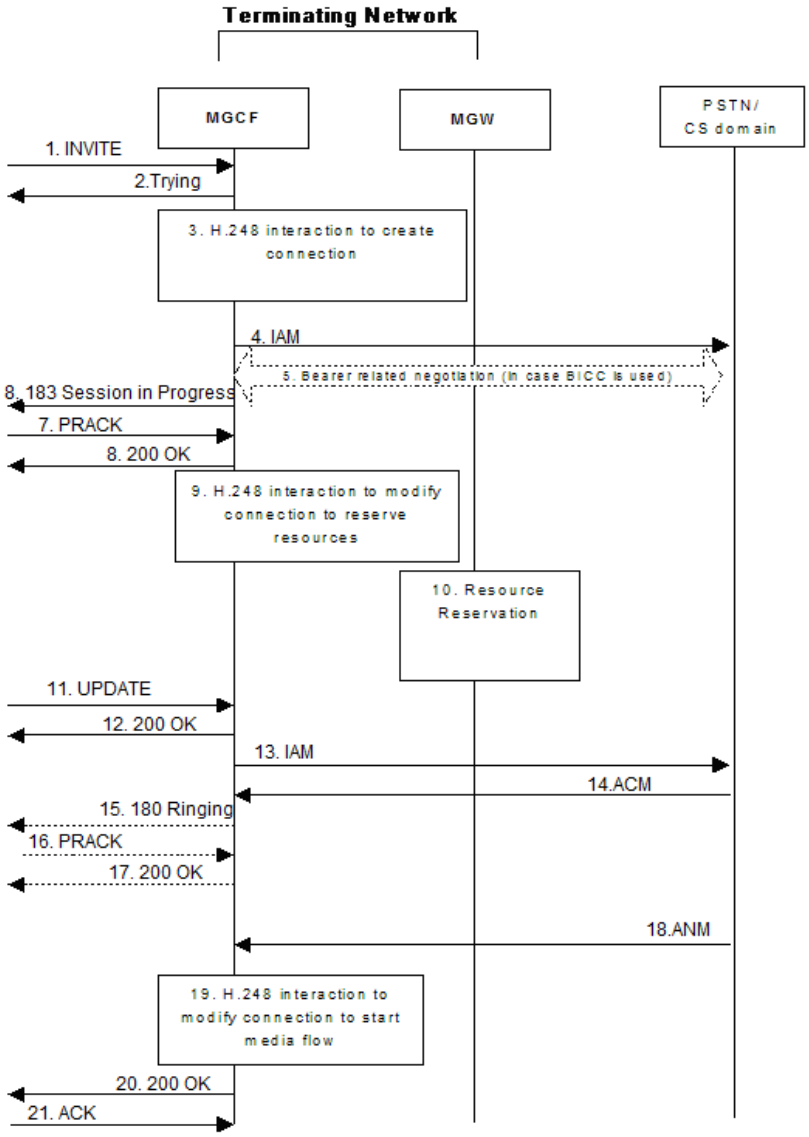

Figura 67. Terminación en la red de conmutación de circuitos

Mensaje 5: Realiza la negociación de medios con el dominio de circuitos si fuera necesario.

Mensaje 6: Llega un mensaje del dominio de circuitos con las capacidades soportadas por el destinatario y el MGCF convierte esto a una respuesta SIP 183 Session in Progress con la correspondiente información de medios.

Mensajes 7 y 8: Si fuera necesario se continuaría negociando los parámetros de la sesión con una segunda oferta en el acuse de recibo de la primera respuesta (PRACK) y su posterior respuesta.

Mensaje 9 y 10: El MGCF da instrucciones al MGW para que inicie la reserva de recursos acordados.

Mensaje 11: El MGCF recibe el mensaje SIP UPDATE con la confirmación de medios reservados por el origen

Mensajes 12: acuse de recibo del mensaje anterior.

Mensaje 13: Envía la confirmación hacia el dominio de circuitos, si hubiera enviado previamente el mensaje IAM (hay soporte de continuidad) ahora enviaría un mensaje COT, si no fuera así enviaría el mensaje IAM por primera vez.

Mensaje 14: Mensaje ACM de la red de circuitos informando que el destinatario está siendo alertado.

Mensaje 15: EL MGCF informa al origen con el correspondiente mensaje SIP 180 Ringing.

Mensaje 18: El MGCF recibe la respuesta final del destinatario ANM

Mensaje 19: El MGCF instruye al MGW para la activación de la conexión entre dominios.

5.6.4.3. Sesión terminada en una red IP externa (No IMS)

Cuando la sesión multimedia tiene como destinatario a un usuario SIP externo que no pertenece a la red multimedia, pueden darse varias situaciones, si el cliente SIP externo soporta las extensiones SIP usadas en la red multimedia, su comportamiento no varía del caso en que el terminal de usuario esté registrado en la red multimedia. Si el cliente SIP del usuario de la red externa no soporta precondiciones entonces los medios negociados sólo estarán disponibles a partir del momento en el que el terminal del usuario IMS tenga los recursos requeridos ya reservados. El diagrama siguiente como se interconecta el terminal externo con la red multimedia.

Mensajes 1-3: Solicitud de sesión multimedia con precondiciones pero indicando que lo medios están desde un primer momento como no accesibles (media =”inactive”).

Mensaje 11: El UE en la red multimedia inicia la reserva de recursos.

Mensajes 12-14: Cuando los recursos están reservados el usuario multimedia inicia la activación y los indica al otro extremo (media = “active”)

Mensajes 15-17: El destinatario acepta la activación de medios y como no tiene que confirmar sus recursos (se da por supuesto que ya están reservados) responde al originador de la sesión permitiendo el acceso a los mismos.

Mensaje 18: El P-CSCF habilita el uso de los medios por parte del usuario.

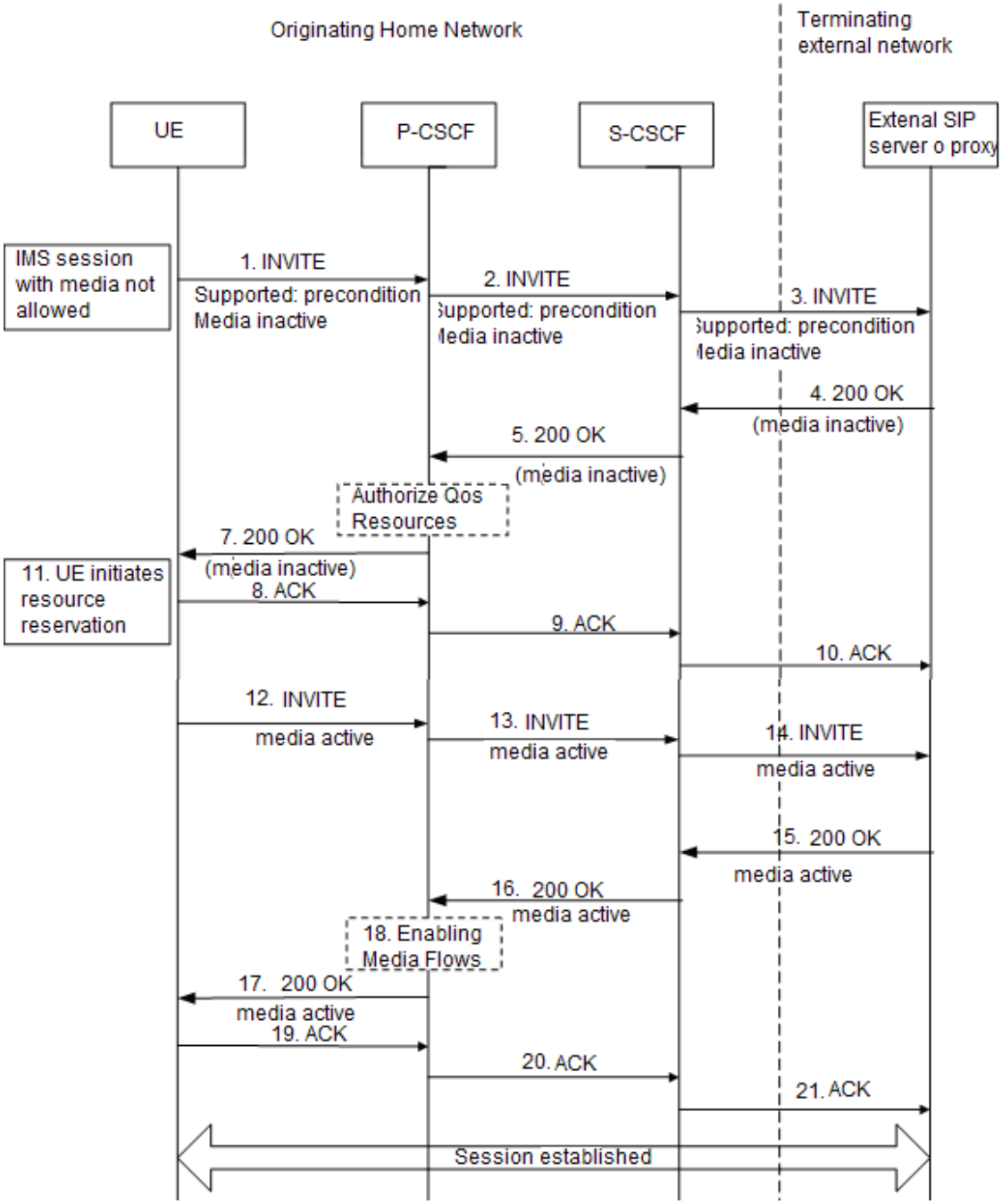

Figura 68. Terminación de sesión en un cliente SIP de un una red externa.

5.7. Flujos de finalización de sesiones multimedia

Los procedimientos de finalización de sesiones multimedia son una parte fundamental de los flujos de mensajes que tiene lugar dentro de una red de comunicaciones. Los procedimientos que explicaremos a continuación tienen como función asegurar la adecuada finalización de la sesión y la liberación de los recursos comprometidos en la sesión en curso. Existen múltiples causas que pueden provocar la finalización de una sesión en curso y pueden ser iniciadas tanto por el usuario como por la red en los casos siguientes:

- Finalización normal de una sesión solicitada por uno de los usuarios finales.
- Finalización de sesión por intervención del operador de la red.
- Finalización de sesión por pérdida de la portadora IP de control de sesión que transporta la señalización de la sesión
- Finalización de la sesión por pérdida de una o más portadoras radio que son utilizadas para el transporte de los mensajes de señalización.

Vamos a considerar tres escenarios, finalización de sesión iniciada por el terminal de usuario de la red multimedia (indistintamente si es el origen o la terminación de la sesión es en la red multimedia o en una red externa), finalización de sesión iniciada por la red multimedia o finalización de sesión iniciada en la PSTN.

5.7.1. Finalización de sesión iniciada por el terminal

En el caso de que unos de los terminales de usuarios, (ya sea el que inició la sesión o el que la recibió) finalizan una sesión voluntariamente se produce un flujo de mensajes a nivel de señalización para ordenar la liberación ordenada de recursos hasta ahora reservados para la comunicación en ambos extremos. Esta situación también es aplicable a clientes SIP pertenecientes a otras redes IP externas. En el caso explicado emplearemos el caso más complicado que es cuando los terminales de usuario se encuentran en roaming en otras redes distintas de sus redes locales. En caso de que uno o los dos terminales se encuentren en su red local, el escenario se simplifica con respecto a este caso como ya se comento en anteriores puntos.

Mensaje 1: Cuando el usuario cuelga y finaliza la sesión, el terminal genera un mensaje SIP BYE y lo envía a la red de acceso y ésta a la red multimedia para la terminación de la sesión.

Mensaje 4: EL P-CSCF recibe la petición y cancela la autorización que previamente había realizado para esa sesión. El P-CSCF indica a la red de acceso que libere los recursos asignados a este usuario para esta sesión.

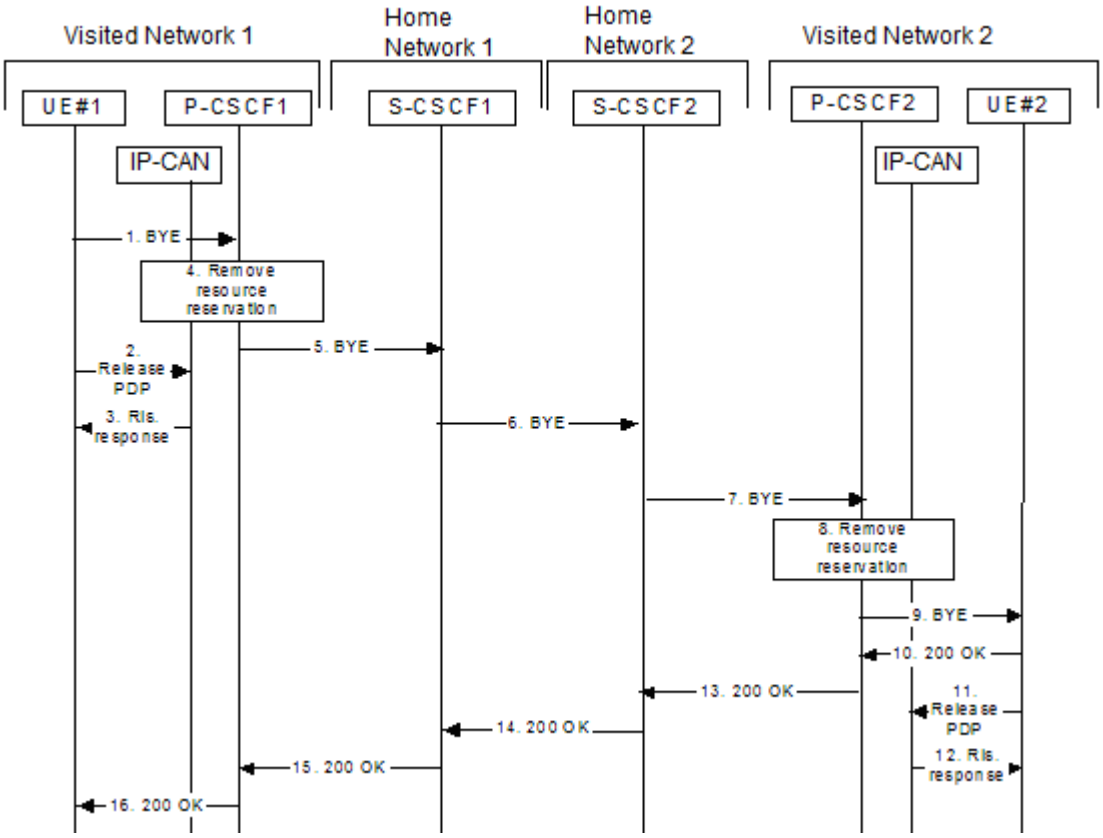

Figura 69. Finalización de sesión iniciada por los usuarios de la red

Mensaje 2: El terminal solicita la liberación de recursos asignado en la red de acceso

Mensaje 3: La red de acceso confirma al terminal y a la red que ha liberado los recursos reservados para esa sesión

Mensaje 5, 6, y 7: El P-CSCF notifica a la red de destino la finalización de la sesión.

Mensaje 8 y 9: Se cancela la autorización de recursos para el usuario de destino y se alerta a la red de acceso para que libere los recursos. Se alerta al terminal que libere recursos también.

Mensaje 10: El terminal de usuario acepta la solicitud de liberación de sesión

Mensaje 11 y 12: El terminal y la red de acceso liberan los recursos actuales.

Mensajes 12, 14, 15 y 16: Una vez que los recursos han sido liberado se notifica a la red y al usuario que finalizo la sesión que el proceso ha concluido correctamente.

5.7.2. Finalización de sesión iniciada por red

La finalización de la sesión también puede ser iniciada por distintas entidades de red (P-CSCF, S-CSCF, AS, HSS) en respuesta a determinadas eventualidades que pueden tener lugar en la red multimedia o en el propio terminal de usuario. Detallaremos los dos casos más frecuentes:

- El punto de entrada en la red local para ese usuario inicia la finalización de la sesión (P-CSCF)
- El punto de control en la red local para ese usuario inicia la finalización de la sesión (S-CSCF)

5.7.2.1. Finalización de sesión iniciada por el P-CSCF

En algunas situaciones la finalización de la sesión no puede ser solicitada por el terminal de usuario (perdida de cobertura, apagado repentino, etc.) y por tanto la red tiene que ser capaz de determinar que ha ocurrido una eventualidad y debe solicitar la liberación de recursos y la finalización de sesión. El siguiente diagrama muestra como se realiza el proceso de liberación iniciado por el P-CSCF.

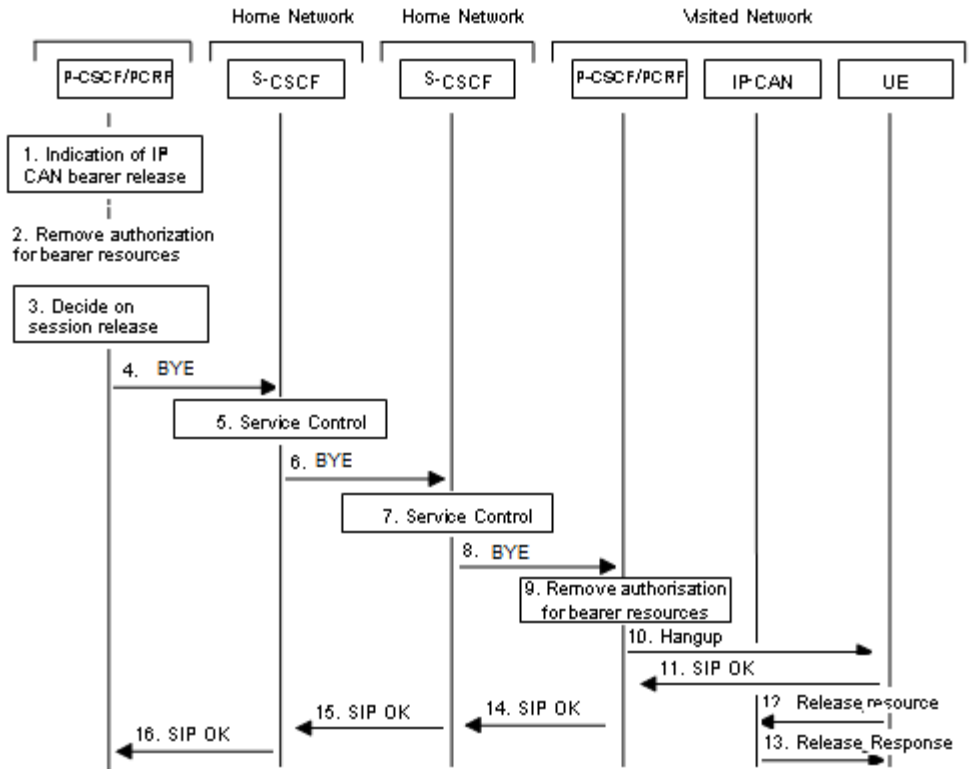

Figura 70.Finalización de sesión iniciada por P-CSCF

Mensaje 1: El P-CSCF recibe información de la red de acceso IP-CAN alertando que se ha perdido la portadora radio que transportaba la señalización o de medios (si esta no ha podido ser reestablecida) para la sesión con el usuario.

Mensaje 2: El P-CSCF suspende el acceso a los recursos previamente comprometidos en la reserva de recursos emitida en el momento de establecerse la comunicación y valora la desactivación de portadoras adicionales en la red de acceso.
Mensaje 3: El P-CSCF determina si es posible reestablecer la portadora de señalización (o las portadoras de medios si estas fueran las afectadas). Si no es posible entonces ordena finalizar y liberar todas las portadoras relativas a la sesión multimedia en cuestión.

Mensaje 4 y 5: El Proxy genera un mensaje de finalización de sesión (BYE) y lo envía al control de sesión para que este lo procese y realice las acciones necesarias.

Mensaje 6: El S-CSCF envía la petición a la red del otro usuario.

Mensajes 7 -9: Procesos equivalentes a los realizados en los puntos 2, 4, 5 y 6 pero en la del otro usuario.

Mensajes 10 y 11: El P-CSCF indica al terminal de usuario que finalice la sesión y este responde afirmativamente.

Mensaje 12 y 13: En paralelo a la respuesta emitida hacia el origen, el P-CSCF o bien el UE (indistintamente) solicitan la liberación de las portadoras asignadas y los recursos de la sesión. En otro extremo responde a la petición cuando éstos se liberan.

Mensajes 14 – 16: Respuesta de confirmación (200 OK) a la finalización de sesión solicitada por el P-CSCF de la red originante.

5.7.2.2. Finalización de sesión solicitada por el control de sesión C-CSCF

Como en el punto 5.7.2.1, el control de la sesión en la red multimedia, puede determinar la finalización de una sesión multimedia actualmente en curso por múltiples motivos (finalización del saldo de un cliente en prepago, orden administrativa de cancelación o modificación de suscripción, por indicación de un servidor de aplicación por expiración de servicio, etc.)

Mensaje 1: El S-CSCF decide finalizar la sesión multimedia del usuario en cuestión (determinado internamente o solicitada por otra entidad de la red)

Mensaje 2: Solicita la finalización de la sesión (Mensajes BYE o CANCEL en SIP) hacia el usuario afectado.

Mensaje 3: El P-CSCF revoca la autorización de acceso a los recursos asignados a esta sesión y solicita la liberación de las portadoras IP asociadas a la sesión en la red de acceso.

Mensajes 4 y 5: El P-CSCF solicita al terminal de usuario que finalice la sesión y que detenga el flujo de medios hacia el usuario remoto y libere lo recursos comprometidos para dicha sesión.

Mensajes 6 y 7: El terminal de usuario responde a la petición anterior con un 200 OK hacia la red.

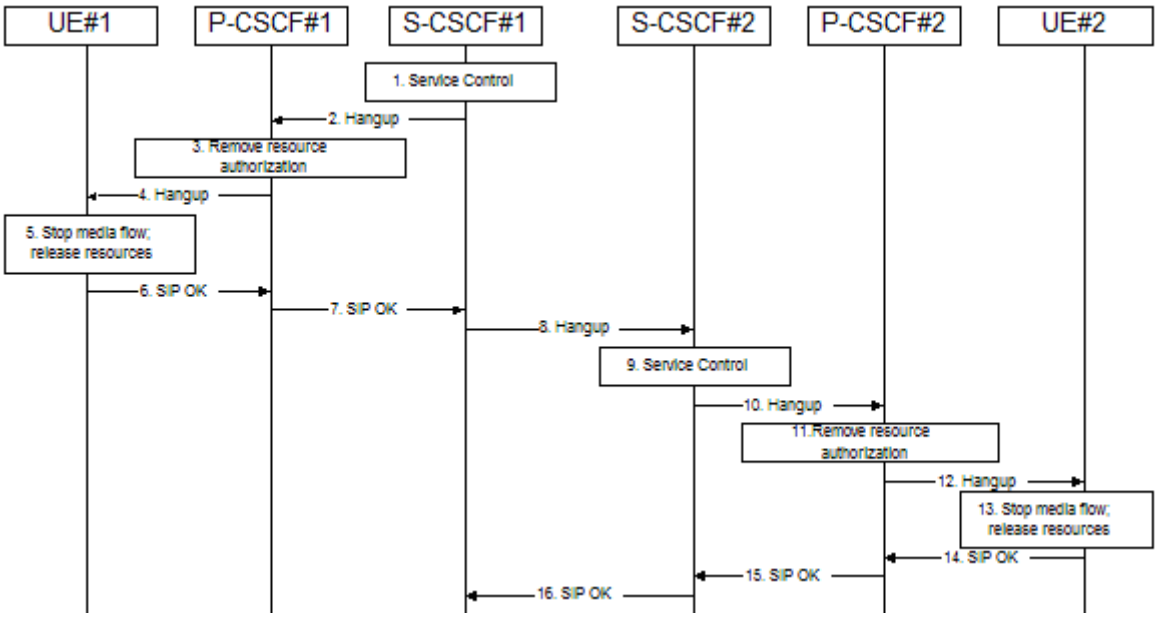

Figura 71. Finalización de sesión iniciada por S-CSCF

Mensaje 8: Al mismo tiempo que el mensaje 2 se indica al nodo de control del usuario remoto la finalización de la sesión.

Mensajes 9 y 10: El S-CSCF del usuario remoto procesa la petición y reenvía la solicita al P-CSCF que se comunica con el terminal de usuario remoto.

Mensajes 11, 12 y 13: Procesos equivalente a los mensajes 3,4 y 5 pero en la red del usuario remoto.

Mensajes 14, 15 y 16: E usuario remoto responde a solicitud de finalización de sesión recibida y reenvía a la red la respuesta para su retransmisión hacia el originador de la finalización de la sesión.

5.7.3. Finalización de sesión solicitada en la PSTN

En el caso de una sesión o llamada entre un usuario de la red multimedia y un usuario de la red pública conmutada (PSTN) el flujo de señalización en el proceso de liberación será el siguiente. En este caso se muestra el flujo de señalización que tiene lugar cuando la finalización se origina en la red pública conmutada. En el caso contrario el flujo seguido sería el mismo que en el punto 5.7.1 con la diferencia que el nodo de control de la red multimedia (S-CSCF) reenvía la petición al MGCF que controla la señalización con la PSTN.

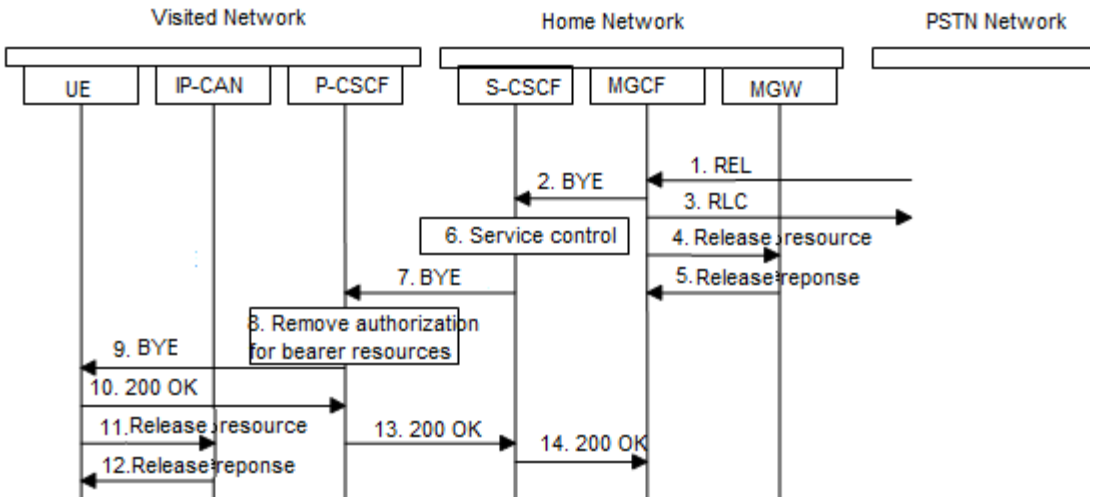

Figura 72. Finalización de sesión iniciada por la red pública conmutada

Mensaje 1: El usuario de la red pública conmutada finaliza la sesión (cuelga la llamada por ejemplo o hay un error en la PSTN que obliga a finalizar la llamada entre otros) se genera un mensaje en REL en ISUP en la red SS7 de señalización de la PSTN que llega al MGCF.

Mensaje 2: El MGCF construye una petición SIP BYE y la envía al control de sesión del usuario multimedia.

Mensaje 3: El MGCF acepta la petición que recibió de la PSTN y contesta con un mensaje RLC (el envío de este mensaje en este instante puede variar en función del tipo de red pública conmutada y posponerse hasta la confirmación de la red multimedia).

Mensajes 4 y 5: El MGCF indica al MGW que inicie la liberación de la conexión establecida entre éste y la red pública conmutada. Cuando la liberación ha sido completada, el MGW responde a la petición del mensaje 4.

Mensaje 6 y 7: el control de la sesión en la red multimedia procesa la petición y genera un mensaje de fin de sesión hacia el terminal del usuario.

Mensaje 8 y 9: El P-CSCF revoca la autorización de recursos asignados a la sesión y envía la petición de liberación de recursos al terminal del usuario.

Mensaje 10, 11 y 12: El terminal confirma la petición e inicia de acuerdo con la red de acceso la liberación de las portadoras IP asociadas a la sesión.

Mensajes 13 y 14: La red confirma que la sesión hacia la red pública conmutada.

5.8. Flujos de redirección de sesiones

La redirección de sesiones es el proceso de redirigir la sesión o llamada entrante hacia un punto distinto del terminal de usuario remoto con el que se pretende establecer la sesión. Este punto remoto puede coincidir con otro terminal de usuario, un buzón de voz o un servicio multimedia.

Normalmente el proceso de redirección de la sesión se produce en algún punto del proceso del establecimiento de sesión pero también puede darse la redirección posterior al establecimiento y los servicios en que normalmente se produce una redirección de sesión son básicamente cinco [26]:

- Redirección de sesión incondicional
- Redirección de sesión variable
- Redirección de sesión selectiva
- Redirección de sesión por usuario ocupado
- Redirección de sesión por usuario sin respuesta

Además la decisión de redirigir una sesión puede ser tomada y realizada por distintas entidades funcionales de la red multimedia y en función al punto de decisión dividiremos las siguientes situaciones.

5.8.1. Redirección de sesión iniciada por S-CSCF

Durante el proceso de registro el S-CSCF que controla al usuario descargará el perfil de usuario de éste del HSS que entre otras informaciones incluirá las condiciones que se tienen que cumplir para activar la redirección de una sesión. Este flujo cumple con los servicios de redirección de sesión incondicional, relativa y variable [26].

Mensajes 1 – 6: El flujo normal en el establecimiento de una llamada en la red multimedia.

Mensaje 7: EL S-CSCF del usuario de destino (S-CSCF#2 en este ejemplo) determina que la sesión debe redirigirse a una nueva dirección SIP URI o TEL URI de destino. Basándose en el perfil de usuario de destino las características de la sesión pueden estar restringidas a las permitidas por éste.

Mensaje 8: El S-CSCF#2 preguntará al I-CSCF a que operador de red pertenece el destino redirigido.

Mensaje 9 y 10: El HSS es preguntado por la dirección del S-CSCF que controla al destino de la redirección (S-CSCF#F)

Mensajes 11: La petición de sesión es dirigida a éste último.

Mensajes 12 y 13: El control de destino redirigido procesa y retransmite la petición de sesión hacia el terminal de destino.

Mensajes 14 – 19: El destino redirigido responde a la petición de sesión y con su oferta de medios soportados hacia el origen de la sesión

A partir de este momento el proceso de establecimiento de sesión continúa como en los casos indicados en el punto 5.6

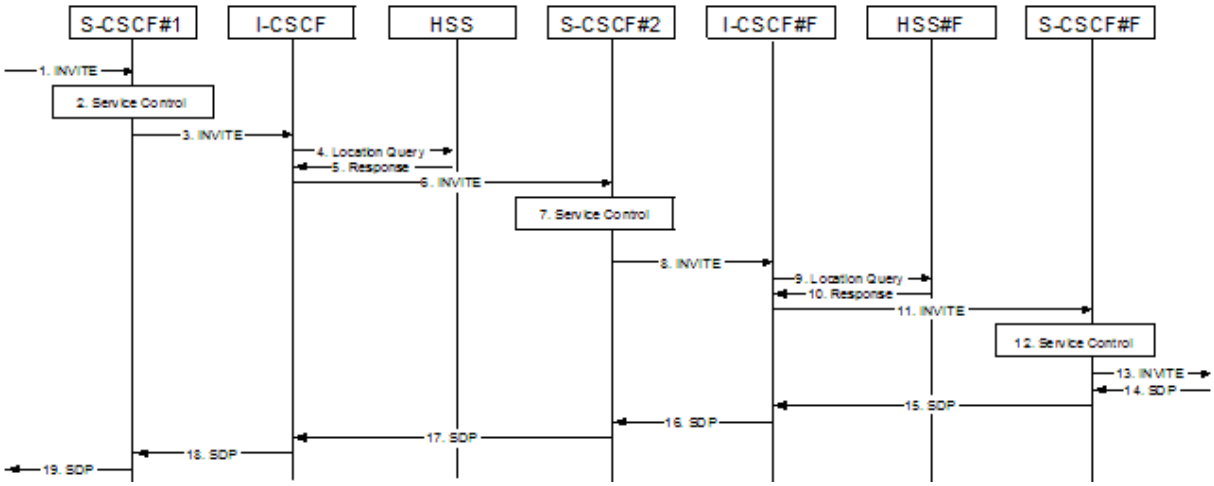

Figura 73. Redirección de sesión en el S-CSCF

5.8.1.1. Redirección de sesión a la red pública conmutada (PSTN) por el S-CSCF

El S-CSCF del usuario de destino determina que la sesión tiene que ser redirija y terminada en un usuario de la red pública conmutada (PSTN) y por lo tanto éste tiene que reenvía la petición de sesión hacia el BGCF de la red para que éste a su vez determine si la interconexión con la red pública conmutada se realiza en esa misma red multimedia o en otra idénticamente a lo explicado en los puntos 5.6.3.3 y 5.6.3.4

En estos escenarios el S-CSCF de destino (S-CSCF#2) permanecerá en el camino de señalización durante toda la sesión realizando el control de la redirección el mismo.

5.8.1.2. Redirección de sesión a la red pública conmutada (PSTN) por la red del usuario de origen UE1.

Este método de redirección es el mismo caso que el explicado en el punto anterior con la diferencia que el S-CSCF#2 determina el usuario de la red PSTN al que redirigir la sesión y se la proporciona al usuario de origen (UE #1) para que éste establezca la sesión directamente con el destino redirigido de acuerdo a los puntos 5.6.3.3 y 5.6.3.4. Para esto empleará el método SIP REDIRECT para proporcionar al terminal de origen la información de la nueva dirección del usuario de la red pública al que solicitar la sesión.

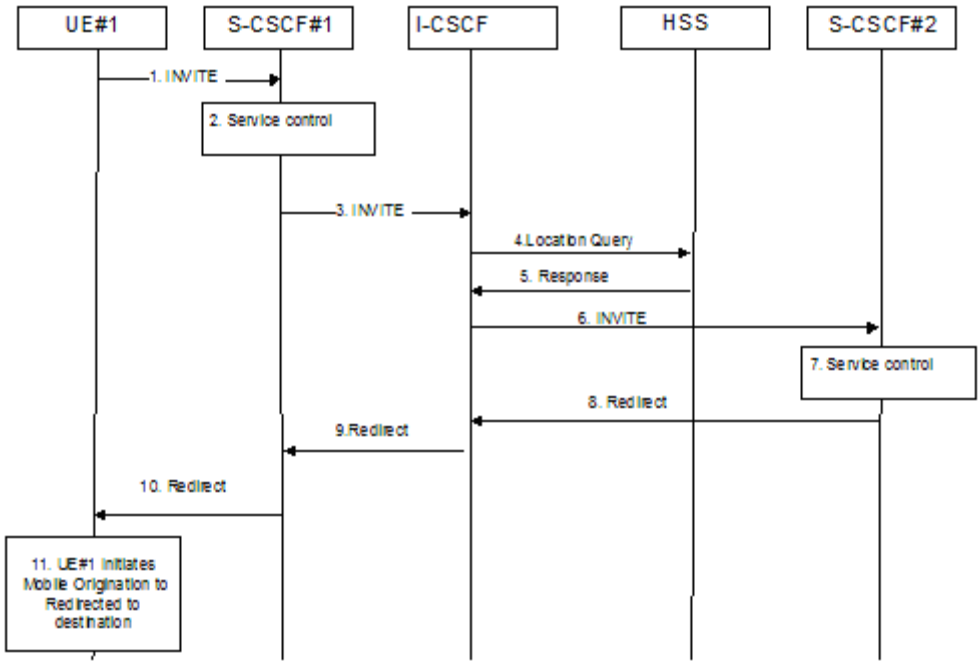

Figura 74. Redirección de sesión a través del usuario de origen

5.8.1.3. Redirección de sesión a un usuario general (fuera de IMS y PSTN)

En este caso la redirección de la sesión se realiza a un usuario que no pertenece al dominio multimedia ni al dominio de circuitos como pueden ser un cliente SIP externo o una aplicación como una página Web, una dirección de correo electrónico, etc. Este escenario es equivalente al punto 5.8.2.1 puesto que la entidad de control del destinatario inicial proporciona al usuario de origen información del nuevo usuario o entidad al que habrá que redirigir la sesión por medio del método REDIRECT.

5.8.2. Redirección de sesión iniciada por el P-CSCF

La entidad que sirve de punto de comunicación entre la red multimedia y el terminal de usuario de destino, P-CSCF también puede determinar la necesidad de un reenvío de la sesión. El P-CSCF es el encargado de hacer llegar al terminal de usuario las peticiones (de sesión en este caso) al usuario y de retransmitirlas hasta recibir el correspondiente acuse de recibo por parte de terminal de usuario.

Si el P-CSCF no se capaz de comunicarse con el terminal (debido a causas como perdida de cobertura repentina, apagado inesperado etc.) éste puede iniciar el proceso de de redirección de sesión indicándole al control de usuario de destino (S-CSCF#2 en este ejemplo) para que éste tome la decisión de a quien redirigir la sesión. La siguiente figura muestra esta situación.

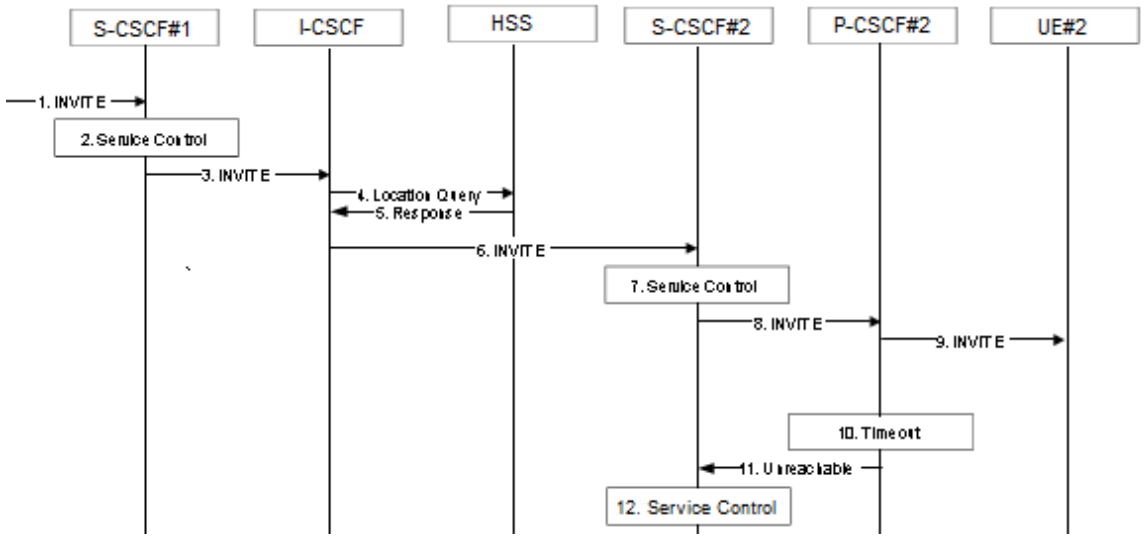

Figura 75. Inicio de redirección en el P-CSCF del destinatario

Mensajes 1 – 8: El flujo normal de mensajes en el establecimiento de sesión entre dos usuarios de redes IMS (la misma red o diferentes).

Mensaje 9: El P-CSCF envía la petición de sesión al terminal de usuario y la retransmite durante un periodo de tiempo hasta recibir respuesta.

Mensaje 10: El P-CSCF agota el tiempo de espera para la respuesta a la petición de sesión y asume que el terminal no está disponible.

Mensaje 11: El P-CSCF envía un mensaje de usuario no disponible al control de la sesión en la red del destinatario.

Mensaje 12: El control de sesión en la red de destino (S-CSCF#2) determina, en base a la información del perfil de usuario, está suscrito al servicio de redirección de sesión o si no es así. En caso de que no sea soportado el control de sesión finalizará el establecimiento de sesión con una respuesta de error hacia la red de origen. Si por el contrario la redirección está activa determinará la nueva dirección URI de redirección (otro usuario, buzón de voz o de correo, pagina web o cualquier otro expresado en formato URI) para continuar la redirección en base al tipo de destinatario redirigido según todos los subpuntos incluidos en el punto 5.8.1.

5.8.3. Redirección de sesión iniciada por el usuario de destino

El terminal de usuario también puede tomar decisiones de redirección de sesión en base a las necesidades especificas de los usuarios como pueden ser en función de la identidad del numero llamante (numero A), si el usuario de destino está actualmente ocupado con otra sesión/llamada/aplicación etc. Por lo tanto

sujeto a las condiciones definidas por el usuario, el terminal indicará en su comunicación a la red cuando desea que se aplique la redirección de una sesión. Los servicios implementados en esta solución son los de redirección variable, selectiva o por usuario ocupado.

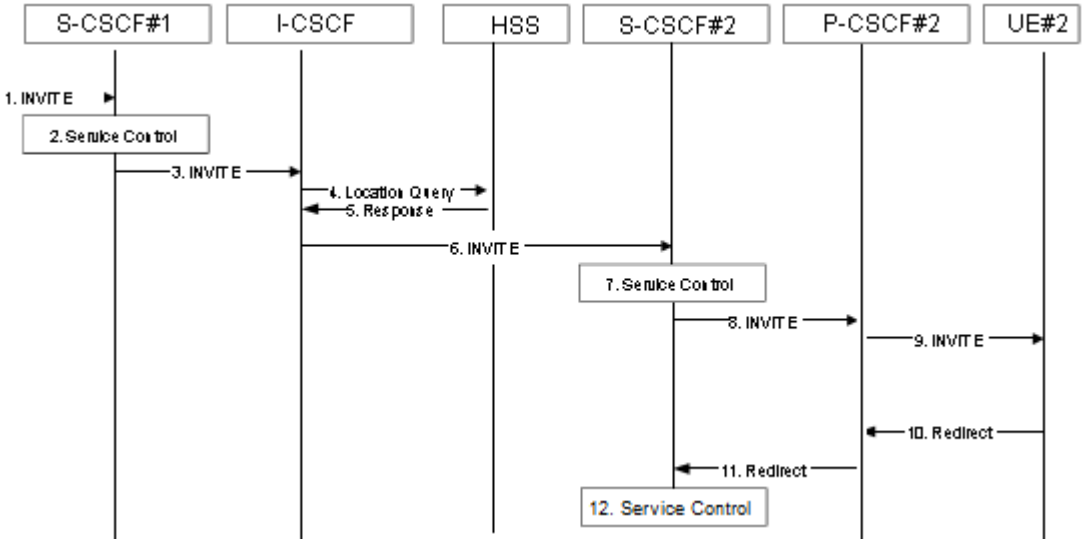

Figura 76. Redirección de sesión determinada por el UE de destino.

Mensajes 1 – 9: El flujo normal de mensajes en el establecimiento de sesión entre dos usuarios de redes IMS (la misma red o diferentes).

Mensaje 10: El terminal de usuario en base a las reglas definidas para ese usuario determina que esa sesión debe ser redirigida y proporciona la dirección a la cual la red debe redirigir la sesión (cualquiera expresada en términos de URI)

Mensaje 11: El P-CSCF reenvía el mensaje REDIRECT al S-CSCF del usuario de destino inicial

Mensaje 12: El control de sesión en la red de destino (S-CSCF#2) determina, en base a la información del perfil de usuario, si el usuario está suscrito al servicio de redirección de sesión o si no es así. En caso de que no sea soportado el control de sesión finalizará el establecimiento de sesión con una respuesta de error hacia la red de origen. Si por el contrario la redirección está activa continuará redirigiendo la sesión hacia la dirección URI proporcionada por el terminal de usuario según todos los subpuntos incluidos en el punto 5.8.1.

5.8.4. Redirección de sesión ya establecida por el destinatario

El este caso la redirección de la sesión puede ser requerida después de que el terminal de usuario del destinatario sea alertado durante un intervalo de tiempo determinado. Una vez transcurrido ese intervalo el terminal del destinatario indica a la red que inicie el proceso de redirección de sesión hacia otro terminal de usuario, un servidor de aplicación, un cliente SIP externo o una

terminación en la red pública conmutada. El servicio implementado en esta redirección es el de redirección de sesión sin respuesta.

El flujo de mensajes es el siguiente:

Mensajes 1- 10: Establecimiento normal de la sesión en la red multimedia y alerta al terminal de usuario de sesión/llamada entrante.

Mensajes 11: Agotado el intervalo de tiempo determinado de alerta al usuario, el terminal de usuario decide que la sesión debe ser redirigida hacia otro usuario (otro usuario en la red multimedia o en una red externa incluida la red pública conmutada) o servicio (servidor de aplicación) o cualquier otro expresado en términos de un URI y se indica al P-CSCF#2

Mensaje 12: El P-CSCF#2 revoca las autorizaciones a los medios previamente autorizados.

Mensajes 14: El S-CSCF#2 determina si el usuario indicado tiene acceso al servicio de redirección de sesiones. En caso afirmativo éste reenvía la petición de redirección (SIP REDIRECT) hacia la red de origen de la sesión. Si este nodo requiere permanecer en el camino de la sesión redirigida, éste sustituye la URI de redirección proporcionado por el UE#2 por una URI privada que apunte a sí mismo. Si no requiere permanecer envía como dirección de redirección la proporcionada por el terminal de destino.

Mensaje 17 y 19: Iguales a los mensajes 14 y 12 pero en la red de origen.

Mensaje 20: El terminal de usuario que origina la sesión, inicia una nueva petición hacia la dirección de redirección proporcionada por la red de destino.

Mensaje 23: Si el S-CSCF#2 de la sesión anterior permanece en el camino de la sesión redirigida entonces la petición se envía a éste, en caso contrario en base a la dirección proporcionada por el usuario se determina que nodo controla al nuevo usuario y el flujo continúa.

5.9. Flujos de transferencia de sesiones

Este procedimiento tiene lugar cuando una sesión establecida entre dos usuarios finales quiere ser transferida por alguno de ellos a un tercer usuario. Para ello se emplea el método SIP REFER sirve para que un usuario indique al usuario opuesto la intención de transferir la sesión por medio de los campos *Refer To* y *Referred By*

Mensaje 2:Durante una sesión establecida el usuario 2 inicia la transferencia de sesión enviando un mensaje SIP REFER incluyendo en campo Refer To en la cabecera con la dirección del usuario al que desea reenviar la sesión y Referred By indicando su propia dirección.

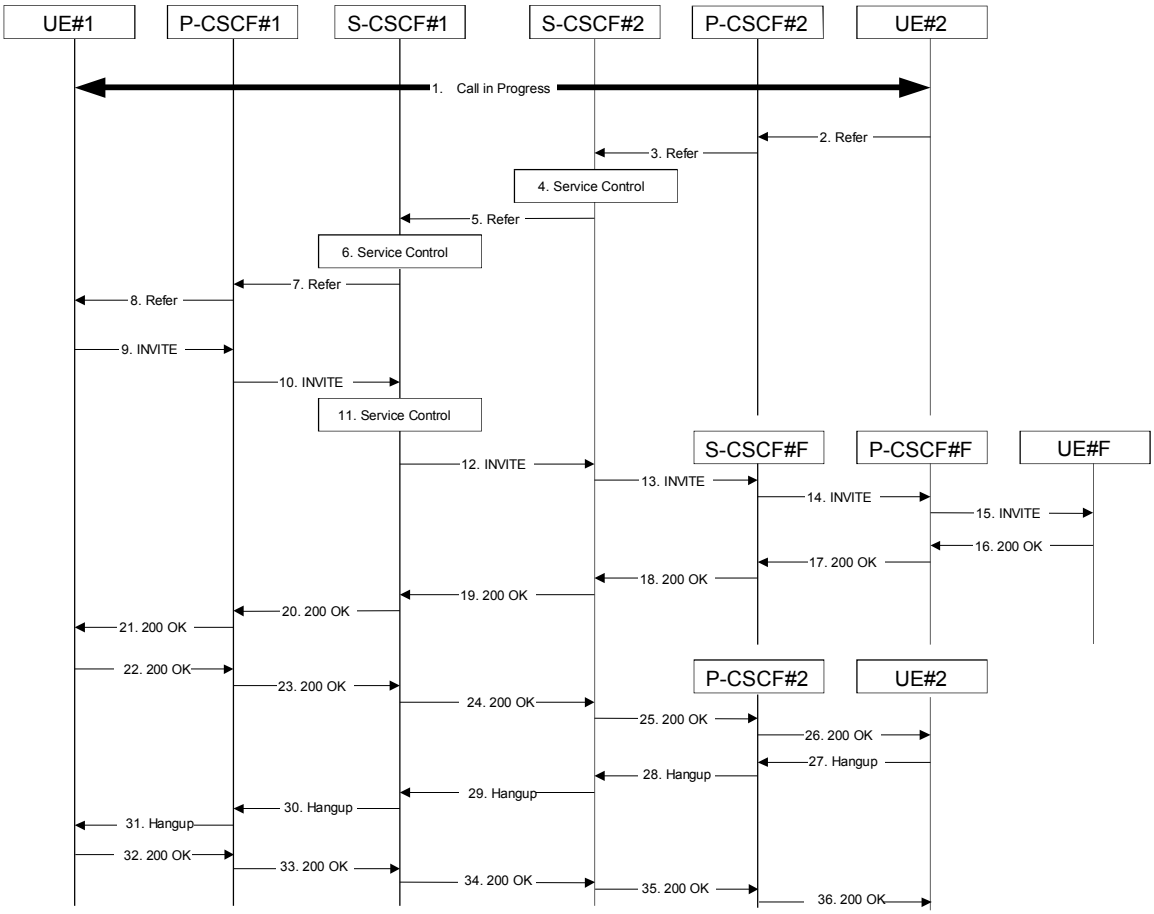

Figura 77. Transferencia de sesión a un tercer usuario iniciada por el usuario de destino

Mensaje 5: El S-CSCF#2 del usuario destino indica a la red de origen su propia dirección en el campo Refer To, ocultando ésta a la red de origen si desea controlar la transferencia de la sesión.

Mensaje 9: El terminal de usuario de origen acepta la operación de transferencia y genera una nueva petición de INVITE incluyendo como destino la dirección del proporcionada por el terminal de usuario UE#2 o por el control de sesión de la misma red.

Mensajes 10 -21: En cualquier caso la petición sigue el mismo camino que un establecimiento de sesión convencional, según los procedimientos del punto 5.6, con la salvedad que lo hará a través de la red 2 siempre que esta desee permanecer en el proceso de transferencia.

Mensaje 22-26: Una vez que la sesión con el usuario transferido se ha establecido, el usuario origen UE#1 contesta a la petición de traspaso REFER originada por el usuario UE#2 con uno 200 OK.

Mensajes 27-36: El usuario que inició la transferencia de la sesión, solicita la liberación de la sesión en curso con el usuario UE#1 con los procedimientos descritos en el punto 5.7.

6. Red troncal móvil de nueva generación. Core de paquetes evolucionado.

6.1. Introducción

Como adelantábamos en el capítulo 1, en las ultimas normas de 3GPP se ha producido cambios muy significativos en las especificaciones para permitir evolucionar a las redes móviles actuales hacia redes de 4ª generación con la introducción de una nueva arquitectura de red basada en una red de conmutación IP única que proporcione acceso a todos los servicios del operador con un nivel de calidad de servicio extremo a extremo garantizado y con plena movilidad entre diferentes tecnologías de acceso inalámbricas y que permitan la evolución hacia redes de comunicaciones móviles de banda ancha mucho más potentes y plenamente interoperables con diferentes redes de servicios IP avanzados, como IMS o Internet [10].

La arquitectura aquí presentada tiene mucho puntos en común con IMS, al compartir muchos de los conceptos desarrollados en esta red de servicios IP, como el concepto de conectividad IP, interoperabilidad con múltiples redes de acceso IP, control de nivel de calidad de servicio extremo a extremo e incluso elementos de su arquitectura como el repositorio de información de usuarios, HSS o los elementos de control de política y tarificación, PCC [10 y 26].

6.2. Características Generales

En este apartado introduciremos brevemente cuales son las principales características en EPC un poco más en detalle.

6.2.1. Arquitectura IP

Una de las características principales de EPC es que introduce una arquitectura mucho más simplificada que las redes precedentes de 2G/3G al eliminar definitivamente el dominio de conmutación de circuitos que existía en éstas y definir únicamente un dominio de conmutación IP que soporta todos los servicios, incluidos los servicios de voz, permitiendo la reducción de elementos en la red troncal y mejorando significativamente los rendimiento por inversión en despliegue y mantenimiento y simplificando los sistemas de gestión y control de la red y reduciendo los costes operativos del operador.

El dominio de datos definido es una evolución de las redes de datos GPRS de las redes 2G/3G a través de una arquitectura IP optimizada y simplificada para el transporte de datos de usuario recibidos desde las redes de acceso, que reduce el número de elementos en la red troncal antes de llegar a la red de servicios IP reduciendo los tiempos de transmisión y procesamiento de la

red y aumentando el rendimiento de la infraestructura y reduciendo los costes [10].

6.2.2. Red multiacceso

EPC es una red troncal multiacceso que proporciona conectividad e interoperabilidad a los terminales de usuario conectados a través a diferentes redes de acceso inalámbricas. Las redes de acceso inalámbricas interconectadas abarcan desde las redes de acceso definidas por 3GPP en las diferentes redes móviles (E-UTRAN, UTRAN, GERAN), hasta redes de acceso inalámbricas de otros grupos u organismos de estandarización (CDMA2000, WiMAX) o redes inalámbricas o fijas genéricas (WLAN, LAN).

Esta integración aunque orientada a conexiones inalámbricas también permitirá la integración con redes de datos cableadas (xDSL, redes corporativas, etc.) para alcanzar la convergencia fijo-móvil más real posible.

6.2.3. Servicios IP

La red troncal suministra a los usuarios de la red conectividad IP a varios dominios de servicios, como IMS o conexión directa a Internet, que serán las plataformas de distribución de servicios multimedia avanzados, que hasta ahora estaban disponibles sólo en entorno de redes de datos cableadas, como telefonía multimedia, servicios de video bajo demanda, servicios de difusión en alta definición (IPTV, HDTV), funciones de computación distribuida en la red (cloud computing), descarga de aplicaciones o juegos en red entre otros y que gracias a la nueva arquitectura de alta capacidad estarán disponibles en un número cada vez mayor de terminales móviles inteligentes.

6.2.4. Funciones de control avanzadas

La red EPC tiene muchas características ya introducidas en arquitectura anteriores y que se han incorporado a ésta con algunas modificaciones que en algunos casos son sustanciales:

- Conexiones extremo a extremo con un nivel de calidad de servicio garantizado. Creación de nuevas clases de nivel de servicio para satisfacer los requerimientos de los servicios de banda ancha en tiempo real más críticos y exigentes.
- Gestión y asignación de recursos de la red a partir de la aplicación dinámica de reglas de política de servicio y control de tarificación definidas por el operador, igual al explicado en el punto 4.6.
- Funciones de enrutamiento y control de tráfico propias de las redes de conmutación de paquetes.
- Procedimientos de control de acceso a la red como autenticación y autorización, control de admisión al terminal de usuario, intercepción legal de señalización, etc.

- Funciones de protección de flujos de datos de usuario a través de mecanismos de encriptación e integridad de datos.
- Escalabilidad. Debido a que los planos de control y de usuario se han separados con entidades lógicas o funcionalidades diferenciadas esto permite que el operador de red pueda hacer evolucionar cada uno de los planos de forma independiente y en base a las necesidades del operador en cada caso.

Y nuevas funcionalidades como:

- Gestión y control de movilidad. La red troncal gestiona y controla no solo la localización de la posición de un terminal dentro de la red de acceso y los traspasos dentro de las zonas de cobertura de esta red de acceso sino que incluye funcionalidades avanzadas que permiten la movilidad y los traspasos de un usuario entre redes de acceso de distinto tipo, Ej. traspasos entre accesos E-UTRAN y WLAN o entre E-UTRAN y UTRAN.

6.3. Arquitectura de red

La arquitectura de red de EPC está basada en la evolución de la arquitectura de las redes GPRS usadas en 2G/3G como mencionábamos anteriormente, realizando una simplificación de la jerarquía de la red separando los caminos que seguirán los flujos de datos de los que seguirán los flujos de control y reduciendo el número de elementos que gestionan cada uno de los caminos con los objetivos de reducir los tiempo de transmisión y procesamiento y aumentar las velocidades de transmisión.

La red troncal está formada por un elemento encargado de todas las funciones de control de la conexión, conocido como MME, en sus siglas en inglés que se encarga de realizar las funciones principales de control de las conexiones de datos de los usuarios y dos elementos del plano de usuario conocidos como S-GW que es la interfaz directa con la red de acceso E-UTRAN y el P-GW que es la pasarela que termina la conexiones de datos hacia otras redes IP. Esta pasarela también es la interfaz de interconexión con el resto de redes de acceso inalámbricas de EPC. A estos nodos hay que añadir algunas funciones adicionales como el repositorio de datos HSS o el control de política y tarificación PCRF. La siguiente figura ilustra la arquitectura global de las redes EPC sin incluir su interconexión con el resto de redes de datos (GPRS/EDGE y pasarelas de conexión a redes de datos externas).

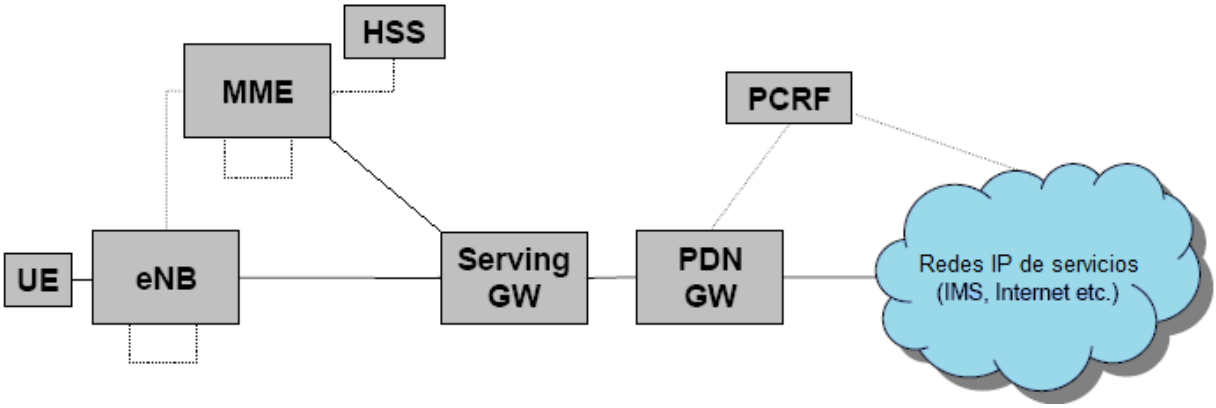

Figura 78. Arquitectura simplificada con las entidades lógicas principales de la red EPS

6.3.1. MME

Es la entidad lógica encargada de realizar las funciones de control y señalización de la sesión de usuario para permiten que el terminal de usuario establezca una conexión de datos con la red. Es la interfaz directa con los nodos de la red de acceso E-UTRAN, e-nodeB, y la interfaz con los elementos de señalización de otras redes móviles como el SGSN de las redes 2G/3G o el PDSN/HA de CDMA.

Realiza funciones de gestión sobre la conexión como la selección de la pasarela de servicio a un usuario y de pasarela de datos para una conexión, mantenimiento de la conexión permanente con la red, control de los recursos asignados por la red, etc. También realiza funciones de control sobre las portadoras de datos de la conexión entre el e-nodeB y la pasarela de datos.

Una de las funciones más importantes que realiza es el control de la localización del terminal de usuario dentro de una red de acceso dada con ayuda de las bases de datos de la red y el soporte del control de los traspasos en las redes de acceso móviles E-UTRAN, UTRAN y GERAN y CDMA2000 con la selección del MME/SGSN/PDSN correspondiente que controla al terminal en cada subsistema de acceso.

6.3.2. S-GW

Es el punto de conexión entre la red de acceso E-UTRAN y la red troncal para la conexión de datos de usuario y se encarga de establecer comunicación con las pasarelas de datos a través de túneles GTP o conexiones PMIP para la retransmisión del tráfico IP del usuario [23.401].

Es también el elemento encargado de gestionar la movilidad en el plano de usuario entre nodos e-nodeB dentro de la red de acceso E-UTRAN y entre ésta y las redes de acceso GERAN /UTRAN enrutandose los paquetes de datos a los nodos de la red radio donde el terminal está conectado a través de túneles GTP para UTRAN/GERAN y E-UTRAN.

6.3.3. P-GW

Es la pasarela que proporciona interconexión con los niveles de servicios (IMS, Internet, redes P2P, etc.) y por tanto el elemento encargado de asignar una dirección IP y parámetros configuración de red al terminal de usuario [10].

Es la entidad encargada de ejecutar la políticas de red del operador proporcionadas por el PCRF del que recibe información a cerca de recursos asignados, control de uso y acceso a los recursos, autorización de nivel de calidad de servicio (clase de calidad de servicio autorizada, tasas de transferencia binarias autorizadas), etc. También realiza funciones de control de tráfico de usuario así como aplicación de tarificación en base a los flujos autorizados y utilizados comunicándose con las entidades correspondientes del sistema de facturación.

Es también la interfaz de interconexión con otras pasarelas de acceso inalámbricas que proporcionan comunicación a través de conexiones PMIP o MIP con la red troncal EPC para redes de acceso no definidas en las especificaciones de 3GPP. Se definen dos tipos de pasarelas, por un lado conexiones no verificadas con la pasarela ePDG para redes WLAN y por otro lado, conexiones verificadas con la pasarela AGW para WiMAX o HSGW para CDMA2000. Además de esto también gestiona el proceso de movilidad en el plano de usuario entre los accesos móviles de 3GPP, GERAN/UTRAN y E-UTRAN y el resto de redes inalámbricas de acceso (CDMA2000, WiMAX, WLAN, etc.), enrutando los paquetes de datos hacia el S-GW para los traspaso hacia las redes de acceso 3GPP desde el resto de redes de acceso y hacia las pasarelas de interconexión ePDG o AGW en el sentido contrario.

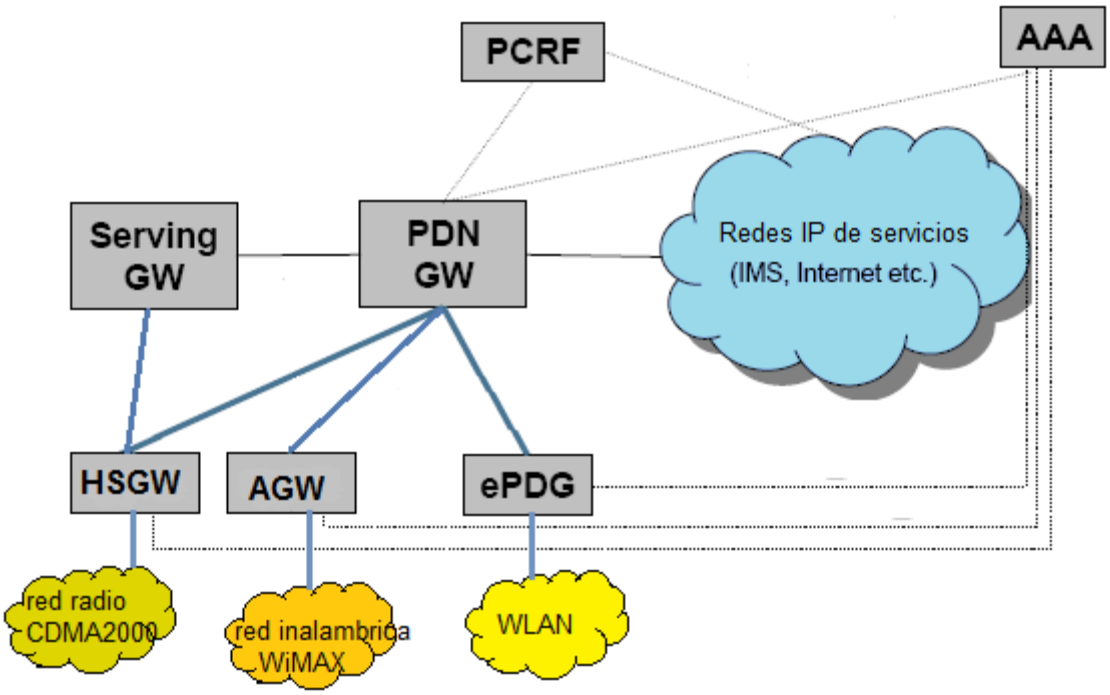

Figura 79. Interconexión con redes de acceso inalámbricas no 3GPP.

6.3.4. PCRF

Es la entidad que como definimos en el punto 4.6.1 realiza el control de calidad de servicio y el control de acceso a los recursos a través de la autorización de recursos de red para cada comunicación, realizando la asignación de parámetros de calidad concretos relativos a cada servicio en base a la política del operador a los recursos disponibles en la red y a los perfiles de suscripción de los usuarios.

6.3.5. HSS

Es el repositorio principal de información de suscriptores en los mismos términos que los definidos en el punto 4.3.1.

6.4. Autenticación, Autorización y control

Estas funciones son realizadas de forma distribuidas por varias entidades lógicas de la red, el HSS, el MME y un servidor de AAA para redes de acceso distintos de las definidas por el 3GPP.
Los procedimientos de autenticación y autorización se realizan a través del procedimiento AKA para aquellos terminales móviles que utilicen alguno tipo de modulo de información del suscriptor (SIM, USIM, ISIM, etc.) puesto que se reutiliza este método de autenticación de estos sistemas y que se gestiona en el servidor HSS definido en IMS. El HSS almacena el conjunto de las claves secretas compartidas y genera un conjunto de información que envía al MME para las redes GSM UMTS y LTE y al servidor AAA para el resto de redes (WiMAX y CDMA2000) para que obtengan información de los terminales de usuario que coincida con la recibida del HSS y autenticar y autorizar a los suscriptores a acceder a los servicios de la red.

Para aquellas redes de acceso cuyos terminales no soporten estos módulos, la pasarela de datos ePDG implementa los mecanismos de autenticación y autorización definidos por la propia red de acceso y el soporta el establecimiento de conexiones securizadas IPsec con los terminales de usuarios para las comunicaciones del terminal.

Las comunicaciones entre el repositorio de los datos de seguridad HSS y los servidores de seguridad AAA y de éstas y las pasarelas ePDG, AGW, HSGW y el MME se realiza a través del protocolo de autenticación, autorización y auditoria Diameter.

6.5. Calidad de servicio

El concepto de calidad de servicio en la red gira entorno al concepto de portadora EPS. Estas portadoras son agrupaciones de uno o varios flujos de datos IP de usuario, utilizados para transmitir el tráfico de datos entre la pasarela de datos y el equipo de usuario cuando se utilizan los servicios de la red. Estos flujos de datos

se definen a través de un conjunto de información en el terminal del usuario y en la pasarela de datos como las direcciones IP de origen y de terminación, los puertos de origen y terminación y un identificador del protocolo empleado en el flujo.

La calidad de servicio es por tanto el conjunto de mecanismos y procedimientos de control y gestión de las portadoras establecidas para cada servicio y el control del nivel de calidad del servicio asignado por el operador [10]. Para ello el operador de red define un conjunto de clases de nivel de servicio que definen unas características de calidad determinadas (tasas de transferencias binarias máximas, garantizadas, ancho de banda reservado, etc.) para cada clase de portadora y que se utilizan para asignarse a cada portadora establecida.

En la red se definen dos tipos de portadoras de servicio, las portadoras por defecto o predeterminadas, que se crean en el momento en que el terminal se registra en la red y que es la que proporciona la conectividad básica con la red la cual tiene asignado un nivel de servicio basado en la información de la suscripción del usuario. Esta conectividad básica le proporciona conexión al resto de redes de datos y por tanto una dirección IP y unos parámetros de configuración para su funcionamiento. Esta conexión a la red dura hasta que el terminal se desregistra de la red y mantiene dicho parámetros de configuración durante todo el tiempo que dura la conexión. Este mecanismo, análogo a los contextos PDP en las redes GPRS, es que permite el soporte de una conexión IP permanente entre la red y el usuario para el despliegue de servicios avanzados que requieren conexión online ininterrumpida.

Complementariamente a éstas se pueden establecer portadoras dedicadas. Estas portadoras dedicadas serán establecidas en base a que son necesarios requisitos de QoS que la portadora por defecto no satisface para un servicio determinado y se necesita establecer una nueva portadora de servicio que si los cumpla. Se pueden establecer tantas portadoras dedicadas como servicios pueda soporta la suscripción de usuario, los recursos disponibles y las políticas del operador.

7. Despliegue e implementación de redes de nueva generación en redes comerciales de operadores.

7.1. Introducción

El concepto de redes de nueva generación ha sido revolucionario dentro de las redes de telecomunicación actuales puesto que ha supuesto un enorme cambio en la forma de en la que se estaban desarrollando las comunicaciones digitales. Este nuevo tipo de redes surge como respuesta a las cambiantes necesidades y demandas de los consumidores de hoy en día y de los innovadores y emergentes servicios impulsados por la explosión definitiva de Internet y de todas las tecnologías asociadas a ésta como medio de comunicación y entretenimiento de masas.

El impulso y desarrollo de los conceptos asociados a las NGNs ha permitido el planteamiento de conectar cualquier usuario/servicio con cualquier usuario/servicio y sobre cualquier acceso/dispositivo/tecnología/red, gracias precisamente al despliegue de esta potente infraestructura de red.

Es por tanto el concepto de NGN como red de comunicación que proporciona una potente plataforma de distribución de servicios avanzados de comunicación el que hace de estas redes la forma más interesante de gestionar los grandes cambios que tendrán lugar en los próximos años en las redes de comunicaciones.

7.2. Consideraciones y contexto de mercado

Los factores relativos a las necesidades, expectativas y demandas de usuarios y las circunstancias y las oportunidades de negocio actuales determinan cuales son algunas características imprescindibles en las comunicaciones del futuro.

7.2.1. Características del mercado

Debido a la adopción de forma masiva por la sociedad de un estilo de vida cada vez más tecnológico, se demanda un mayor acceso a contenidos digitales de banda ancha desde cualquier lugar (movilidad) y desde cualquier dispositivo (teléfonos móviles inteligentes, tabletas, ordenadores portátiles, PCs, PSTN etc.…) y todo ello con una elevada calidad de servicio en un entorno donde los consumidores desean obtener todos esos beneficios al menor coste posible.

La situación actual del mercado de las telecomunicaciones impone unas condiciones exigentes debido al contexto de crisis económica mundial, donde los operadores tienen que ajustar y reducir sus costes de mantenimiento y operación a la vez que aumentan la rentabilidad y productividad de sus inversiones en

nuevos despliegues para poder mantenerse competitivos y no ser expulsados del mercado.

A pesar de que el mercado de las telecomunicaciones siempre ha sido un mercado altamente competitivo y las empresas están habituadas a esta situación, a las condiciones antes expuestas se une una nueva amenaza, la irrupción de desarrolladores de servicios de comunicación por Internet. A causa del fuerte desarrollo de Internet como nueva plataforma de comunicación, en los últimos 15 años han aparecido multitud de competidores que desarrollan aplicaciones y funcionalidades de comunicación a través de Internet de una forma muy rápida y a costes muy bajos, que permiten que éstos sean distribuidos de forma gratuita o a precios mínimos para los consumidores y que ponen en serio peligro los modelos de negocio de los operadores de telecomunicaciones empujándoles a convertirse en meros canales de transmisión si no son capaces de evolucionar y proporcionar nuevos servicios de valor añadido que les permitan competir con estos.

7.3. Planteamientos de la industria

Por tanto es necesaria la definición de una hoja de ruta a seguir por los operadores de telecomunicaciones para adaptarse a las nuevas condiciones del mercado y que permita a los operadores afrontar la cuestión existente en la industria de si permanecer en las capas más bajas de la red como mero medios de distribución para los servicios avanzados desarrollados por terceros o convertirse en plataformas de servicios multimedia avanzados y como llevarlo a cabo. Existen diferentes puntos de vista dentro de la industria de cuál es el mejor camino para la implementación de los conceptos asociados a las redes de nueva generación.

7.3.1. Implementación de una plataforma NGN/IMS

Parte de la industria considera que la mejor solución a largo plazo a todos los retos antes mencionados pasa por crear una plataforma multimedia de gestión y control común e independiente del nivel de acceso para la creación, desarrollo y distribución de servicios avanzados IP propios y de terceros en condiciones de movilidad, continuidad y calidad de servicio cuyo resultados serán un aumento de los ingresos, una importante reducción de los costes de operativos y de distribución y por lo tanto una ventaja competitiva sobre el resto de operadores o desarrolladores.

7.3.2. Implementación sin NGN/IMS

Otra parte de la industria considera que lo realmente importante de las redes de nueva generación es el desarrollo de los conceptos asociados a éstas y no tanto la infraestructura y las entidades lógicas que conforman la red y defienden que los conceptos que hay detrás de la redes de nueva generación pueden alcanzarse por medio de la combinación de subsistemas estandarizados

independientes, soluciones propietarias de fabricantes, plataformas de distribución de contenidos y su integración a través de APIs y pasarelas de conexión.

7.4. Proceso de implementación

7.4.1. Estado actual de las redes de comunicaciones

Centrándonos en las redes de comunicaciones móviles, con la llegada de la 3ª Generación móvil la mayoría de los operadores móviles migraron el nivel de transporte de las redes GSM hacia un nivel de transporte y distribución sobre IP o ATM. Sin embargo este mismo cambio no se llevó a cabo en la redes de acceso en la misma medida, provocando que todavía hoy en día el proceso continúe abierto y solo con la llegada de LTE como estándar de acceso 4G se concluirá definitivamente. A pesar de estos avances en las redes troncales y de acceso de transporte, la mayoría de los operadores móviles todavía mantienen desplegada una red de señalización basada en SS7 y todavía no ha empezado a migrarse hacía una red SIP/IP. El ejemplo de IMS es bastante claro, su implementación real en las redes actuales está lejos de completarse puesto que los operadores de telecomunicaciones no han visto la necesidad de avanzar hacia la integración de un nivel de control IP hasta que se han empezado a trabajar sobre redes de acceso de banda ancha 4G en el último par de años.

7.4.2. Proceso de transformación

La migración de todos los niveles de la red de un operador (las redes de transporte troncales y de acceso, los nodos de señalización, los servidores de aplicaciones y servicios, las interfaces de comunicación con servicios externos o desarrollados por terceros,…) va a ser un proceso largo y gradual que estará marcado por múltiples factores y se dirigirá la sustitución o introducción progresiva equipamiento IP (por antiguos equipamientos en caso de sustitución) que soporte la nueva infraestructura. Partiendo de las redes troncales de distribución de fibra óptica desplegada actualmente, la aparición de la banda ancha móvil de 4G en las redes móviles, llevará a la transformación de los elementos de red convencionales por otros que se comuniquen de forma nativa sobre IP con los dispositivos finales de los usuarios por medio de sesiones de datos. No menos importante durante todo este proceso será el desarrollo y despliegue de diversas pasarelas de interconexión (tanto a nivel de transporte y como de señalización) que actuarán como puntos de enlace entre el nuevo dominio y los dominios existentes de un operador de red permitiendo la comunicación entre usuarios que no pertenezca a la misma red.

7.5. Situación actual de NGN y las tecnologías asociadas

Las especificaciones y los estándares básicos para las redes de nueva generación están disponibles desde hace años como vimos en el capítulo 1.4 (a partir de las Release 5 y 6 de 3GPP) sin embargo su constante evolución y mejora y el continuo incremento de características adicionales (continuidad de sesiones entre dominio, etc.) han provocado que la industria no se haya lanzado todavía a desarrollar productos técnicos completos. A pesar de esto se han desarrollado algunas características concretas descritas dentro de las especificaciones que han sido implementadas en subsistemas independientes, integrados posteriormente en las infraestructuras de red a través de APIs y sistemas de integración [41]. La existencia de esta alternativa para obtener las posibilidades de una NGN con la ayuda de sistemas de integración que permiten la conexión a plataformas de distribución de contenidos y servicios a través de API´s y pasarelas de comunicación , reducen significativamente el volumen de inversiones que se requieren y aunque con limitaciones y no todas las características nativas de una infraestructura NGN completa, permiten ofrecer servicios y aplicaciones que cumplen con las necesidades de los usuarios (distribución multimedia en múltiples formatos y dispositivos).

La situación económica actual como indicábamos en el punto 7.2.1 ha servido de freno también para el despegue de estas redes que a pesar de disminuir y mejorar las inversiones necesarias para su despliegue respecto a las redes convencionales, requiere todavía una importante inversión de desarrollo y despliegue por parte de fabricantes y operadores.

Es en resumen la falta de madurez de las implementaciones técnicas, la magnitud y complejidad del proceso, la existencia de alternativas que requieren menores inversiones, unido a los problemas económicos actuales, los factores que están posponiendo o interrumpiendo el despliegue de las infraestructuras asociadas cuyos resultados a medio–largo plazo no son vistos como prioritarios frente a los resultados a corto plazo de los negocios actuales de la industria.

8. Solución de interconexión IMS para la red de Orange España

8.1. Introducción

Vamos a centrar nuestro caso práctico en el piloto desarrollado por Ericsson AB para la red de comunicaciones móviles del operador móvil Orange en España (France Telecom).

8.1.1. Antecedentes: MSS

Ericsson desarrolló al inicio de la década pasada una solución para dar respuesta a las especificaciones introducidas en la release 4 de 3GPP relativa a la redes de 3G que incorporaban nodos de conmutación no monolíticos donde por primera vez aparecía el nivel de transporte y conmutación de la red troncal separado del nivel de señalización y control de la misma.

Esta separación permitió múltiples beneficios, que ya explicamos más detalladamente en el punto 1.5, tanto a nivel de control como a nivel de transporte, permitiendo la introducción de un nivel de transporte IP que redujo significativamente los costes de mantenimiento y operación con respecto a los nodos de conmutación monolíticos.

El MSS se definió como la agrupación de dos tipos de entidades funcionales, por un lado, uno o varios nodos de control y señalización, denominados MSC Server, que se encargaban de gestionar la señalización de control de las llamadas en la red troncal móvil por medios de los protocolos de señalización BICC o ISUP con otras MSC Server de red o con los subsistemas de acceso (BSS). Y por otro lado una o más entidades en el nivel de transporte llamados MGW, que actúan como nodos de conmutación de la red de trasporte de la red móvil que transporta la información de los usuarios a través de TDM, ATM o IP (dependiendo del tipo de transporte desplegado) dentro de la red. La siguiente ilustración muestra la solución implementada por Ericsson para la ruptura de las antiguas estructuras monolíticas de la red separando precisamente estas funcionalidades en las dos entidades propuestas.

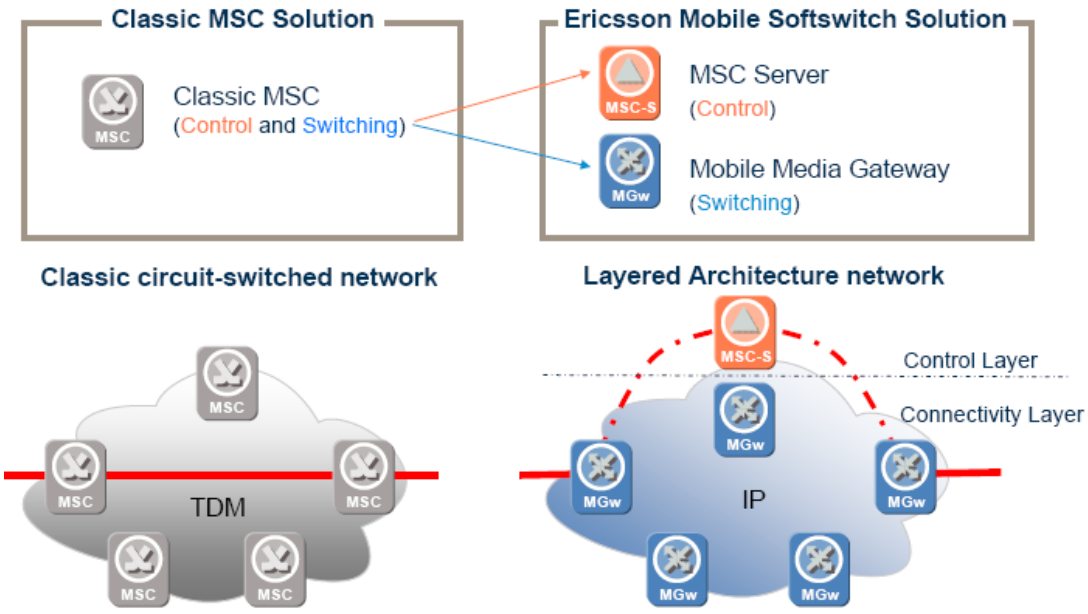

Figura 80. Solución no monolítica de Ericsson. MSS

8.2. Solución de interconexión

Ericsson propone como solución de integración e interconexión para las redes móviles actuales (3G y 2.5G) con la red multimedia IMS, el aprovechamiento de su solución MSS adaptándola a los escenarios de nueva generación por medio de la incorporación de nuevas funcionalidades que permiten que actúe como nodo de interconexión entre la red móvil y la red troncal IMS.

La solución MSS como decíamos estará compuesta por dos elementos funcionales, una en el nivel de control, el MSC-S, que es el resultado de la combinación de las funciones desarrolladas por el MSC Server como nodo de conmutación de las redes móviles y de la entidad funcional MGCF como nodo de interconexión del nivel de señalización de la red multimedia, y otro elemento en el nivel de transporte, el M-MGW, que funcionará como una pasarela de medios entre la red multimedia IMS y la red móvil convencional. MSS será por tanto el responsable de gestionar todo el tráfico de VoIP entre la red móvil convencional y la red multimedia.

El MGCF es como explicábamos en el punto 4.5.1.1 la entidad de control para la interconexión con redes externas que además de gestionar la llamada o sesión entre dominios, controla las operaciones correspondiente en las pasarelas de medios MGW entre la red móvil y la red multimedia.

El M-MGW incluido en la solución MSS, es un híbrido de la pasarela de medios MGW, utilizada en las redes de transporte móviles de 3G y la pasarela de medios IM-MGW, para las redes de transporte multimedia. Su objetivo principal es permitir interconectar dos redes de transporte de dos dominios diferentes para la transmisión del tráfico de usuarios entre ambos dominios. Los M-MGWs están bajo el control del MSC-S/MGCF que controla todo el proceso a través de la interfaz estandarizada Mc/Mn utilizando los protocolos GCP/SCTP.

En la siguiente figura introducimos la solución propuesta por Ericsson para interconectar ambas redes.

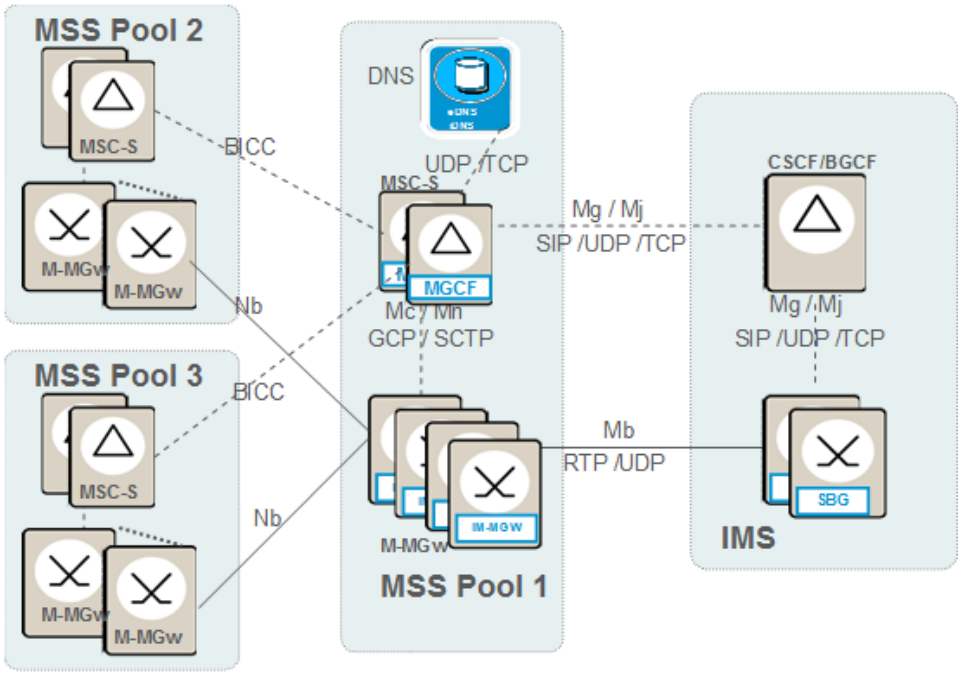

Figura 81. Solución de interconexión entre la red móvil y la red multimedia

Esta solución simplifica y abarata el escenario de migración de las redes móviles convencionales hacia la red multimedia y permite el aprovechamiento de las arquitecturas MSS actualmente desplegadas e integradas plenamente con el resto de subsistemas del dominio móvil de Orange (BSS, OSS, EMA etc.) adaptándolas para que actúen como MGCFs y IM-MGWs de interconexión con la red multimedia.

8.2.1. Configuración de MSS

En la solución propuesta cada MSS está basada en la solución MSS 5.1 por al menos por dos MSC Server R13.2 modificadas para actuar como MGCFs. El despliegue dentro de la red de Orange se realizará con 3 MSS, con un mínimo de 6 MSC-S/MGCF y 7 emplazamientos para las MGWs [43].

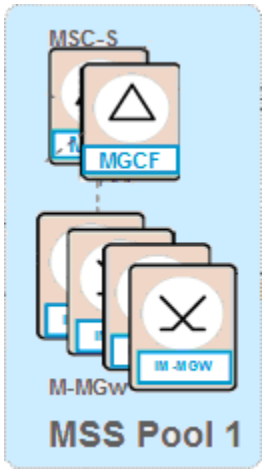

Figura 82. Configuración del MSS para la red multimedia

8.2.2. Contextos de despliegue

Esta solución de interconexión puede desplegarse en varios escenarios, como nodo de interconexión entre la red multimedia y la red móvil convencional de un mismo operador de red, como nodo de tránsito para interconectarse con redes multimedia de diferentes operadores u otras redes móviles desplegadas sobre IP.

8.2.2.1. Interconexión entre dominios del mismo operador

Cuando la interconexión se realiza entre el dominio multimedia y el dominio móvil actual. Desde el punto de vista de la red multimedia el MGCF proporciona una interconexión hacia una red de conmutación de circuitos y desde el MSC-S la interconexión se ve simplemente como un trunk o conexión SIP estándar. Por otro extremo el MSS se comunica a través del MSC-S con el MSC Server de la red móvil por medio del protocolo BICC o con los subsistema de acceso radio con protocolo propios (RANAP/BSSAP). Por lo tanto el MSC-S/MGCF realiza funciones de control de llamada entre dominios y adaptación de protocolos de control (RANAP/BSSAP/ISUP/BICC ←→ SIP) hacia cada dominio.

El MSC-S/MGCF instruye y controla a los nodos del nivel de transporte que transmiten la información de los usuarios por la red. En la siguiente ilustración se muestra como el MSS entre ambos dominios de comunicación.

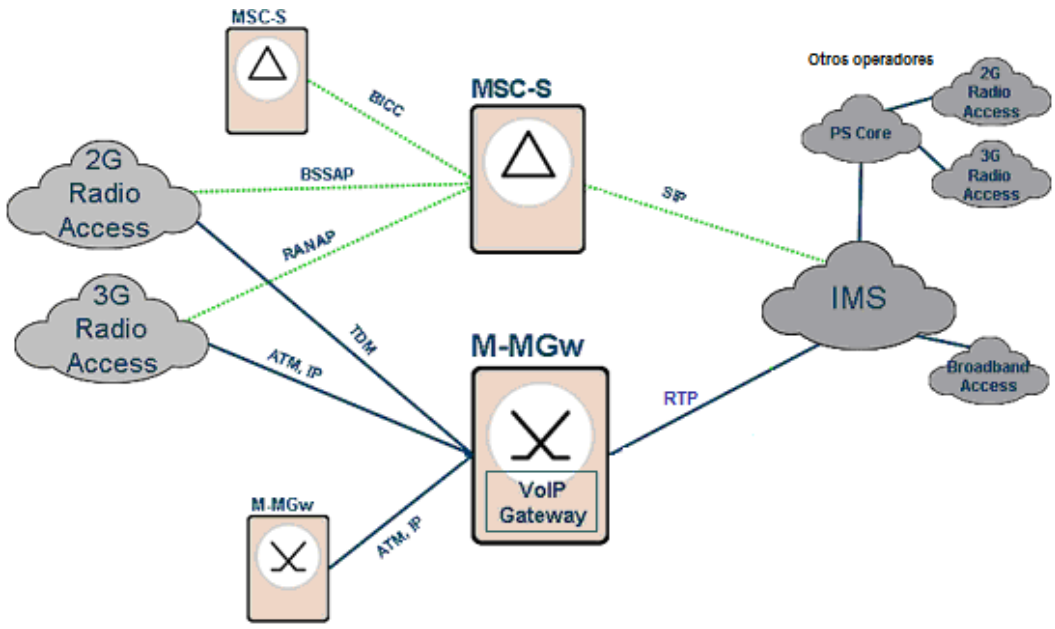

Figura 83. Interconexión entre dominio 3G-IMS de un operador

8.2.2.2. Interconexión de tránsito

La otra posibilidad es el que el dominio móvil de Orange se interconecte con el dominio multimedia o con otro dominio IP de otro operador. Cuando la interconexión se realiza entre dominios IP no es necesario la adaptación de protocolos de señalización y transporte por tanto el MGCF realiza únicamente las funciones de control de llamada y de flujos de sesión entre dominios. En este caso donde el nivel de transporte sigue siendo IP entonces en lugar de emplear SIP como señalización se utiliza la variante SIP-I que a diferencia de la versión estándar incluye una copia de los mensajes ISUP/BICC de la red de origen (si esta es la red móvil o cualquier otra red SS7) como parte del cuerpo del mensaje SIP y lo retransmite encapsulado en un mensaje SIP-I que cuando llega a la red de destino se desencapsulan y se utilizan como mensajes de señalización en dicha red de destino. Esta operativa tiene lugar en redes donde la señalización SS7 se estructura sobre redes IP, como es el caso de SIGTRAN.

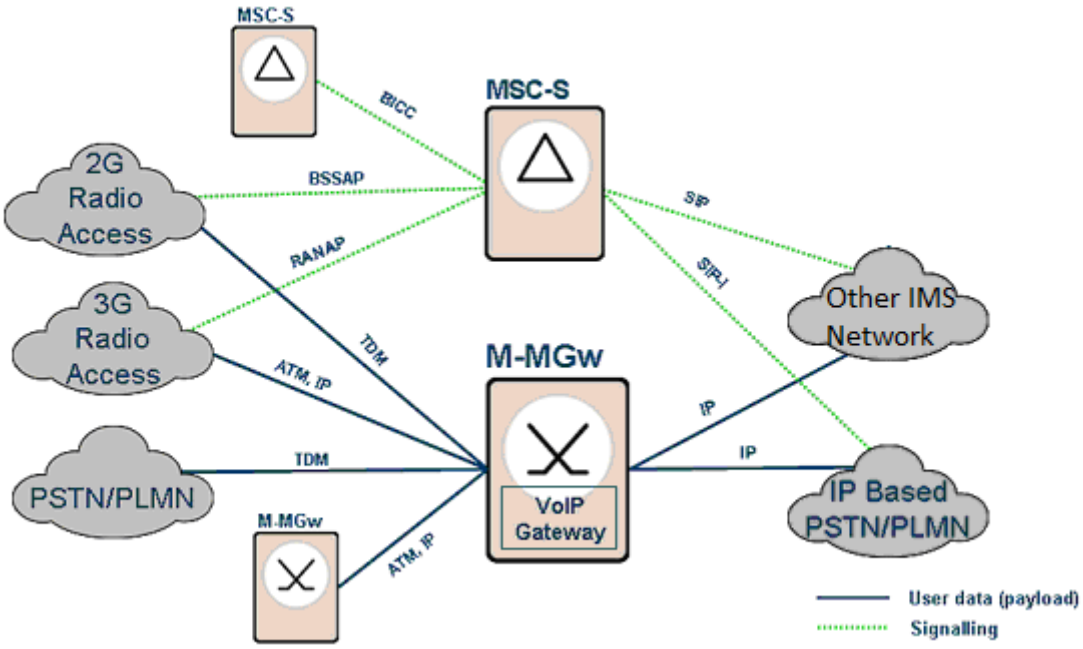

Figura 84. Interconexión entre dominios de distintos operadores

8.2.3. Funciones en el nivel de control

Detallaremos cuales son las principales funciones realizadas por la solución propuesta dentro del nivel de control.

8.2.3.1. Configuración del nivel de transporte

El MSC-S permite el uso de los protocolo UDP y TCP de transporte para señalización SIP y determina como se configuran las sesiones SIP entrantes y salientes.

8.2.3.1.1. Sesiones entrantes

Pueden configurarse dos modos:

- El MSC-S crea dos sockets o conexiones, uno en TCP y otro en UDP que estarán escuchando las peticiones que provengan de los dominios autorizados cuando el operador desee soportar ambas opciones.
- El MSC-S crea una única conexión TCP que escucha las peticiones entrantes deshabilitando las conexiones UDP.

Independientemente del modo seleccionado se implementa un mecanismo de supervisión sobre las conexiones establecidas para determinar si funcionan correctamente o si se producen caídas o errores y generar las correspondientes alarmas en el sistema de supervisión (NMS) al que se encuentran conectados los MSC-MGCF y activa el mecanismo de reconexión automática que intenta una nueva conexión a los puertos definidos cada 5 segundos hasta que lo consigue o es desactivada la activación del puerto por el operador.

8.2.3.1.2. Conexiones salientes

Cuando define los parámetros de enrutamiento que veremos a continuación indica por medio de un parámetro configurable como quiere establecer el transporte para llamadas salientes.

En este caso el MSC-s puede determinar si realiza la salida por TCP, UDP o ambos en base al tipo de mensaje que desee transmitir. Si el mensaje a transmitir es menor a 200 octetos entonces utiliza UDP como protocolo de transporte mientras que para mensajes grandes utilizará siempre TCP.

8.2.3.2. Enrutamiento

La decisión de enrutamiento se determina en base a un número de destino (numero B) junto con información del suscriptor, de la ruta de entrada de la sesión (información del camino recorrido hasta el nodo). Todo ello forma parte del análisis de enrutamiento realizado en el MSC-S y dará como resultado una ruta de salida definida por el conjunto de nodos físicos y lógicos que tendrá que seguir la transmisión desde ese MSC-S en adelante hacia el destino.

La información de cada ruta está compuesta por:

- Conjunto de información de ruta (RSI)
- Información de configuración de conexión SIP (SCI)
- Perfil de versión ISUP encapsulada (EIVP)

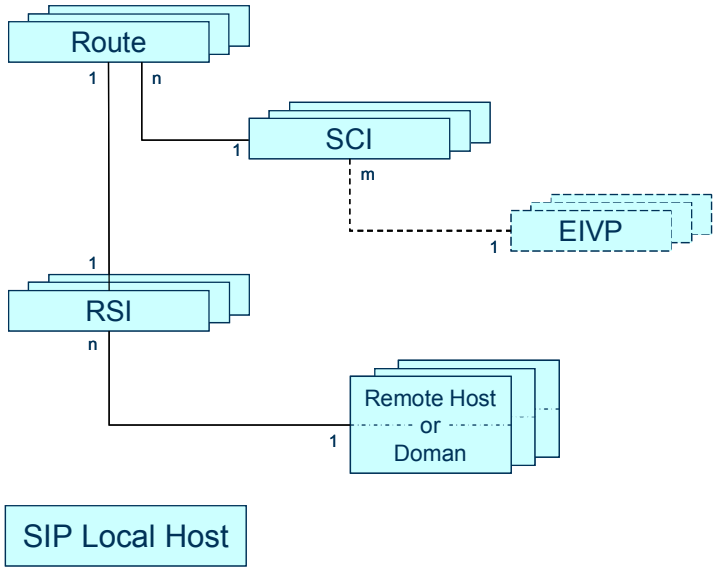

Figura 85. Estructura de decisión de enrutamiento.

8.2.3.2.1. Conjunto de Información de ruta (RSI)

Es un conjunto de información que representa la dirección de destino y la de origen, siguiente salto en el camino y el dominio de destino.

Los campos que forman este grupo de información son:

NHOP: Dirección IP o de dominio del próximo salto en el recorrido.
DEST: Dirección IP de destino.
SRC: Dirección IP o dominio del origen de la llamada/sesión. Utilizado para discriminar el origen y obtener información de la red de origen, extraer parámetros asociados de la ruta SIP de entrada, etc.
DOMID: Nombre de dominio de la red SIP de destino. Si no se proporciona información de NHOP entonces se utilizan los mecanismos NAPTR y SRV de DNS para determinar los protocolos de transporte y las direcciones IP necesarias para llegar hasta el destino.

8.2.3.2.2. SCI y EIVP

SCI proporciona información de la variante SIP (SIP-T y SIP-I) que deberá ser utilizada en la llamada SIP de salida del nodo y por tanto como debe construirse las peticiones SIP hacia la red externa. La variante SIP-I incorpora el una copia de los mensajes BICC/ISUP dentro del cuerpo del mensaje SIP mientras que SIP o SIP-T solo hace un mapeo entre SIP e ISUP.

El EIVP proporciona información de la versión de ISUP utilizada por la red de conmutación de circuitos. Este campo es opcional y solo se requiere cuando en el SCI se indica el empleo de la variante SIP-I.

8.2.3.2.3. Discriminación de llamadas entrantes

El MSC-S/MGCF solo acepta llamadas entrantes al dominio multimedia que provengan de redes de origen conocidas. Para ello las direcciones IP de destino o de origen, los nombre de los servidores remotos y el dominio remoto configurados en el MSC-S y en la información RSI deben coincidir con la información recibida en las cabeceras SIP (cabeceras Via que aportan información del origen de la llamada/sesión) recibidas de otros nodos SIP adyacentes. Solo en este caso se permitirá la llamada y en caso contrario será rechazada. Por lo tanto la información (Direcciones IP o nombres de equipos) insertada en la petición inicial enviada por el origen tiene que estar coordinada con el resto de nodos SIP de la red.

8.2.3.2.4. Distribución de tráfico hacia otros dominios

La inclusión del mecanismo de discriminación por origen limita el uso y las ventajas de utilizar servidores de dominio DNS, puesto que esta función requiere que se indique la mayor cantidad de información posible (nombres, direcciones IP, rutas) para determinar el origen de la llamada, en oposición a la ventaja principal de DNS que es reducir este tipo de información todo lo posible.

Una forma de contrarrestar esto es combinar el uso de la resolución de nombres con consultar SRV. Incluyendo estas consultas (se pregunta al servidor de resolución por un dominio y este devuelve el nombre de un servidor de servicio) cualquier nombre de servidor que pertenezca a un dominio dado puede ser almacenado en la configuración del MSC-S y cumplirá con el proceso de discriminación.

8.2.3.3. Control de carga y protección contra sobrecarga

El MSC-S está protegido por un mecanismo de control de carga donde el MSC-S cuando se encuentra bajo condiciones normales acepta peticiones de inicio de sesión (SIP INVITE) para nuevos diálogos SIP (o SIP-I) y mensajes SIP OPTIONS aislados. Cuando el nodo está bajo sobrecarga las peticiones INVITE de inicio de sesión para nuevos diálogos y mensajes fuera de diálogos son rechazadas con respuesta de servicio no disponible (SIP 503 Service Unavailable).

8.2.3.4. Negociación de codificación en el plano de usuario

El MSC-S se encarga de gestionar la negociación de codificaciones hacia cada dominio, por un lado el MSC-S negocia con la red móvil y por otro lado el MGCF negocia con la red multimedia. Esta negociación se realiza de forma independiente hacia cada dominio y no impide la aplicación de la funcionalidad TrFO (usado para evitar transcodificaciones innecesarias cuando el códec negociado hacia cada red es el mismo) La excepción en la negociación

independiente se produce cuando un extremo el negocia el codec G.711 y el MSC-S/MGCF está obligado a negociar la misma codificación en la otra red.

8.2.4. Implementación física del MSC-S

Desde la Release 5.1 de los MSS los MSC-S (Release 13) disponen de un modulo IP en el procesador central (CP) de la central de conmutación que proporciona conectividad IP para el soporte de SIP y DNS en las MSC-S. Las implementaciones utilizadas para este piloto en IMS están basadas en los sistemas APZ utilizados en las soluciones AXE y más concretamente en la versión APZ 212 50 [40].

8.2.4.1. Conectividad en MSC-S

Este sistema de procesamiento de alta capacidad permite la gestión de un elevado número de operaciones de comunicación de entrada-salida con la red IP externa a través de dos interfaces o tarjetas físicas GigaEthernet que componen el nivel de conectividad del modulo IP de procesador central del sistema. La conectividad de estas dos interfaces físicas no se realiza directamente desde estas hacia el exterior si no que por motivos de protección de la unidad de procesamiento se interconectan cada una de ellas a una tarjeta GESB que a su vez se conectan a un par de switches externos que proporcionarán protección contra sobrecarga de tráfico y envío de tráfico malicioso hacia el sistema aumentando el nivel de estabilidad, seguridad y redundancia del MSC-S.

Además de la redundancia física conseguida con las dos interfaces de red del modulo IP se define una interfaz lógica sobre cada interfaz física asignadas cada una a la misma VLAN, las cuales tendrán configuradas una o varias direcciones ip lógicas flotantes que en caso de caída de la interfaz definida como primaria se activarán inmediatamente en la interfaz secundaria como mecanismo de redundancia lógica.

El procesador central APZ 212 50 tiene una limitación máxima de 2048 canales lo que se traduce en que permite un establecimiento máximo de hasta 200 llamadas por segundos.

La siguiente figura ilustra la arquitectura de la MSC-S empleada.

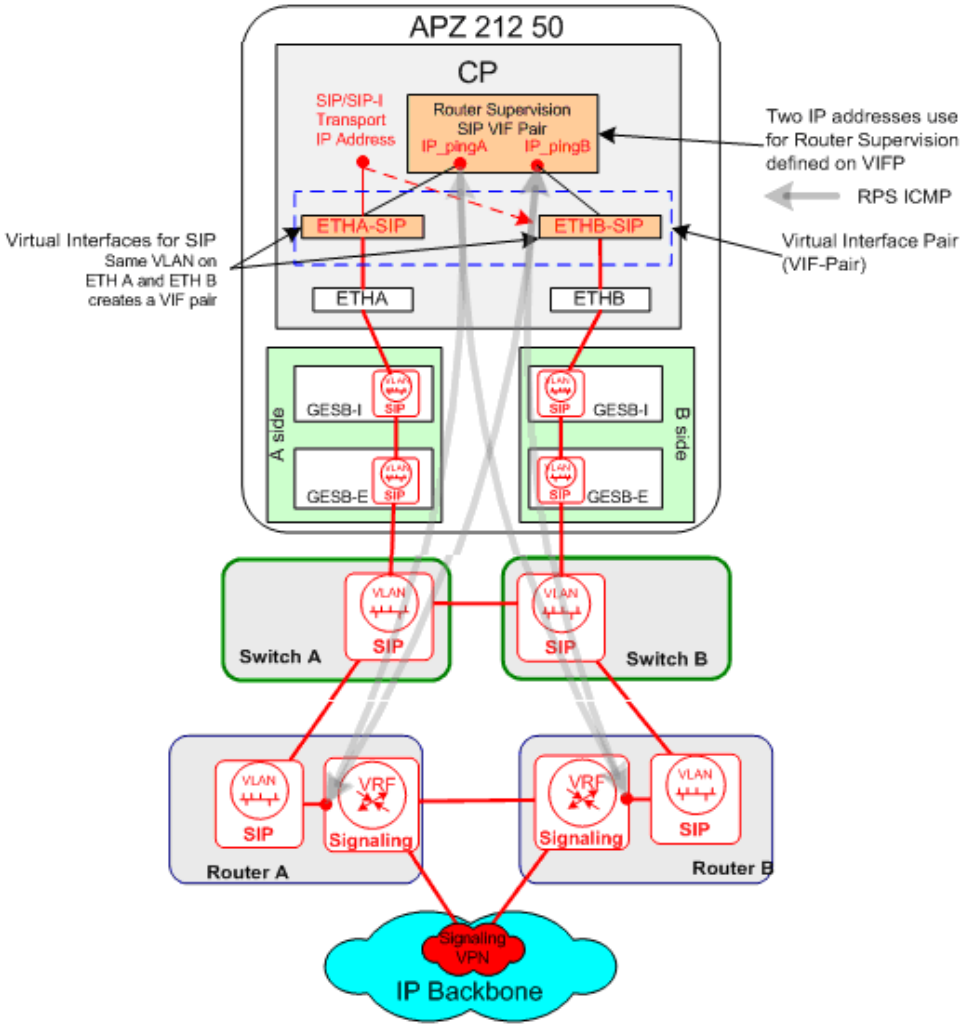

Figura 86. Implementación física y lógica del MSC-S

8.2.5. Funciones del nivel de transporte

El conjunto de capacidades y funcionalidades disponibles en el M-GW para la interconexión en el plano de usuario son las siguientes.

8.2.5.1. Adaptación de protocolos/tecnologías en las portadoras de tráfico

El M-MGW soporta la transmisión de portadoras de diferentes tecnologías como portadoras de transporte de la información de usuario. Hacia el dominio móvil el M-GW soporta la transmisión de tráfico de usuario sobre portadoras TDM, celdas ATM y tramas IP en función de las tecnologías desplegadas en la red de transporte móvil convencional del operador y soporta el envió de tramas IP hacia el dominio multimedia. En caso de interconexión de dos dominios de transporte con tecnologías diferentes realiza operaciones de adaptación.

8.2.5.2. Transcodificación en codificaciones incompatibles

Permite convertir la codificación de los mensajes de usuario entrantes de uno de los dominios de transporte a una codificación soportada por el otro dominio en caso de incompatibilidad de codificaciones.

8.2.5.3. Control de tasas de transferencia hacia cada sentido

Controla y adapta la velocidad de transmisión hacia cada red de transporte según la tecnología y los parámetros determinados por cada uno. Realiza control de flujos determinando el estado de carga en la red.

8.2.5.4. Interoperabilidad DTMF

Soporta la transmisión de información asociada a los pulsos DTMF desde el dominio de circuitos al dominio multimedia adaptando estos en los mensajes de señalización de SIP para permitir conservar las funcionalidades típicas de los dominios de conmutación de circuitos como anuncios, locuciones, funciones IVR etc.

8.2.5.5. Transporte de paquetes de usuarios en el códec negociado

El MSC-S/MGCF permite que si el códec negociado por el usuario origen con la red es soportado y coincide con el negociado por el usuario de destino, la información de usuario se transporta codificada sobre ese mismo códec a lo largo de toda la red sin necesidad de realizar cambios de codificación en ningún punto (función TrFO).

8.2.5.6. Transporte de paquetes de usuario comprimidos sin transcodificación

Soporta el mecanismo de transmisión de voz comprimida montada sobre una trama PCM para su transmisión entre M-MGW de la red troncal evitando la necesidad de hacer transcodificación en la red (función TFO).

8.2.5.7. Funcionalidades IP

Con respecto a las redes de transporte IP soporta identificación de redes virtuales, diferenciación de calidad de servicio entre llamadas y control de admisión de tráfico [40] entre otras funcionalidades avanzadas de la red multimedia.

8.2.6. Transmisión en el plano de medios

8.2.6.1. Codificaciones soportadas

El conjunto de codificaciones soportadas en el M-MGW implementado es:

- GSM-EFR Para redes móviles con un tiempo de paquetización de 20 y 40 ms.
- AMR (set1 modos 0,2, 4, 7) con intervalos de señal de 20 y 40 ms.
- AMR-HR (set1 modos 0, 2, 4) con intervalos de señal de 20 y 40 ms.
- PCM (G711) de 5 a 40 ms en salto de 5ms.
- G729 entre 10 y 40 ms con satos de 10 ms.

8.2.6.2. Transmisión hacia otras redes IP

Cuando la red multimedia de transporte se interconecta con otras redes de transporte IP el MSC-S/MGCF establece que la transmisión de información se realice con el códec G729 (Si no existe ninguna incompatibilidad en la sesión) hacia otros dominios IP puesto que este códec es válido en cualquier red SIP y ofrece una consumo optimo de ancho de banda y un elevado nivel de compresión sin pérdida significativa de calidad.

El M-GW seleccionado en cualquier caso permite el uso de los códec AMR, EFR, G729 y G711 para las codificaciones de los paquetes RTP.

8.2.7. Implementación física M-MGW

La implementación física de los M-MGW para la red multimedia está basada en la solución MGW Release 6 (Releases 6.1 y 6.2).El MGW está conectado a dos interfaces físicas GigaEthernet que proporcionan conectividad a dos switches y dos routers para conectarse a la red troncal IP (backbone) de Orange. Estas duplicaciones físicas permiten establecer redundancias físicas 1:1 para cada M-MGW. Sobre la misma interfaz física se definen las interfaces Mb (para trafico IP hacia el dominio multimedia) y Nb (hacia la red core IP móvil) definiéndose las mismas funciones de transporte para ambos casos.

9. Solución de integración IMS en la red de Orange España

9.1. Introducción

Este capítulo describe la solución de IMS implementada por Ericsson AB para Orange España a partir de la infraestructura previa de IMS para Orange de otro fabricante.

El objetivo fundamente es proporcionar una plataforma multimedia para ofrecer servicios de voz hasta a un millón de usuarios residenciales a través de conexiones de datos ADSL.

9.2. Consideraciones globales

La solución propuesta por Ericsson será implementada como una arquitectura de red redundada y distribuida en múltiples localizaciones geográficas configuradas en modo activo de tal forma que los nodos desplegados en una única localización puedan asumir el tráfico global de la red en caso de fallo del resto de nodos.

La integración del subsistema multimedia de Ericsson se realiza tanto en las redes IP, las redes de conmutación de circuitos, el subsistema de control de negocio (BSS) y el subsistema de operaciones (OSS).

9.3. Arquitectura de la solución

La arquitectura propuesta por Ericsson es la solución IMS MMTel 11A que incluye nodos en los 3 planos propios de las arquitecturas de IMS:

- en el plano de servicios

  Los servidores de aplicación y servicios MTAS 11A

- En el plano de control

  Los servidores de control de la sesión o llamada CSCF 11A, HSS 11A

- y el plano de conectividad o transporte

  Compuesto por routers y switches para la transmisión del tráfico de señalización y del tráfico de usuario y las pasarelas de medios MGW y los nodos de medios MRFP 11A que transmiten el contenido de las

sesiones en la red y permiten la interoperabilidad en el plano de usuario entre diferentes tecnologías y formatos.

Además de esto proporciona funciones externas de gestión y asistencia de la red como DNS/ENUM, provisión por EMA, etc. La figura 86 incluye una visión general de la arquitectura de red:

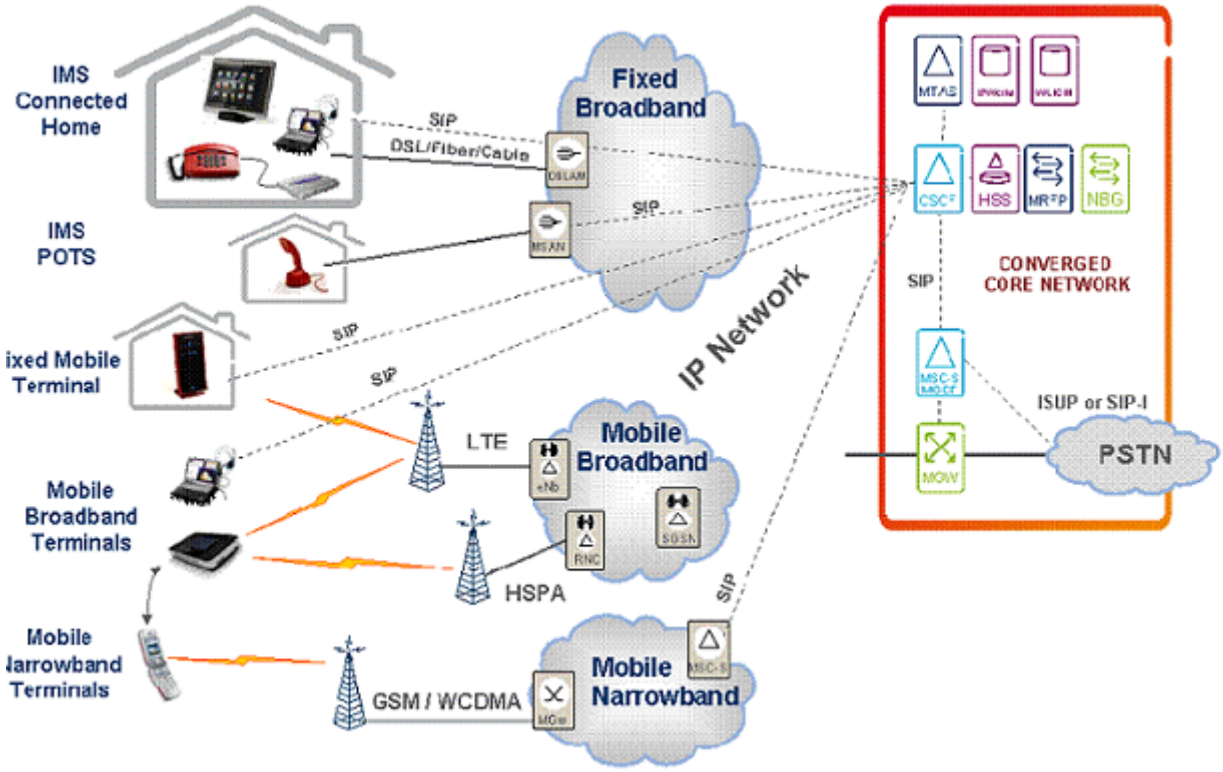

Figura 87. Integración plataforma IMS en redes de acceso actuales

9.3.1. CSCF

Como se ha explicado ampliamente en el punto 4.2 de este documento, los nodos CSCF conforman el corazón del control y gestión de las sesiones multimedia que se establezcan en la red.

En la solución implementada por Ericsson para Orange España se implementa el nodo CSCF 11A basado en la plataforma TSP6.0 implementada sobre el hardware NSP5.0 o 6.0 con características de capacidad y almacenamiento mejoradas.

En función de la entidad que se desea implementar se configurará la plataforma para dar lugar a las diferentes entidades de control (I-CSCF o P-CSCF o S-CSCF o E-CSCF) incluso se podrá soportar nodos de análisis de enrutamiento externos (BGCF, BCF). En base a las necesidades del operador la configuración de entidades puede realizarse o de forma aislada en plataformas TSP/NSP distintas o bien integrando varias entidades en un único nodo como se puede apreciar en la siguiente ilustración.

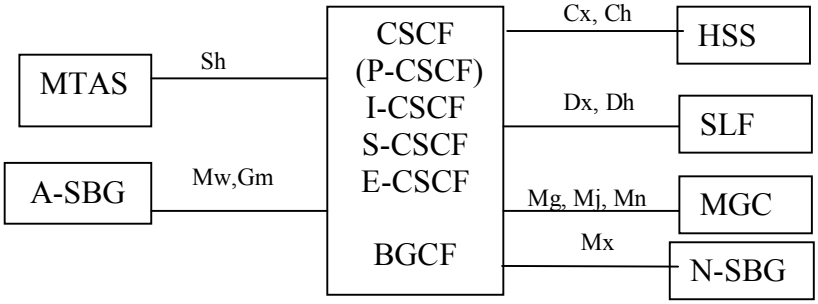

Figura 88. Diagrama de CSCF e interfaces basado en plataforma TSP

9.3.2. HSS

Introducido en el punto 4.3, es la base de datos central del sistema que alberga toda la información de las suscripciones de usuario y de servicios y por tanto tiene una importancia crítica en el despliegue de la red multimedia.

Puede funcionar en dos modos diferenciados. El modo clásico como base de datos maestra que alberga toda la información de los perfiles de los suscriptores y que proporciona dicha información a los MTAS y CSCF para su uso o bien puede configurarse como nodo de interacción y gestión (front-end) con el resto de la red donde la base de datos de suscriptores como tal se encuentra en otro servidor externo (o back-end) de donde el HSS obtiene la información.

Independientemente del modo de configuración el HSS diferencia entre dos tipos de información:

- Información relativa al perfil de usuario del suscriptor, como la definición de cada perfil, características de los servicios, etc. almacenada con el formato y la estructura propios del HSS. Este tipo de información es accesible por los niveles de servicio y del control pero cuya gestión estará bajo el subsistema de provisión EMA.
- Información específica de usuarios y de servicios propia del nivel de aplicación (MTAS). El HSS almacena esta información sin conocer su formato y estructura.

El nodo configurado, realiza todas las funciones explicadas en el punto 4.3 como identificación, AAA a partir de todos los mecanismos de autenticación explicados en los puntos 3.2.4.4 y 3.2.4.5, facturación, localización de usuarios y S-CSCF donde está registrado, bloqueo, comunicaciones con el nivel de servicio y el nivel de control etc.

9.3.2.1. SLF

Como explicábamos en el punto 4.3.2, en el caso de redes de comunicaciones que por su tamaño y por el volumen de suscriptores a manejar necesitan desplegar más de un HSS, se hace necesaria la incorporación de la entidad SLF. Dicha función se implementa en el mismo nodo que el HSS y su función varía según el modo de funcionamiento de HSS.

9.3.2.1.1. SLF con HSS en modo clásico

El SLF, puede actuar de dos formas, o bien proporciona la dirección del HSS donde está alojado el perfil del usuario o servicio para que la entidad que lo solicita (CSCF, MTAS, etc.) y éste envié una nueva petición Diameter al HSS en cuestión o bien el proprio SLF retransmite la solicitud de información hacia el HSS seleccionado en nombre de la entidad de control o servicio.

9.3.2.1.2. SLF con HSS en Modo interacción

El SLF en este caso se comporta como un balanceador de carga entre los HSS implementados que actúan de front-end de la base de datos final.

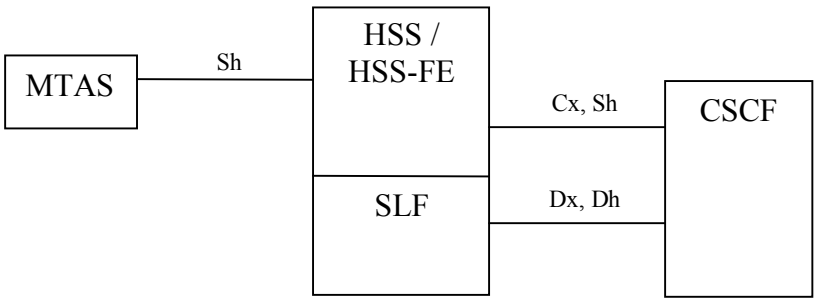

Figura 89. HSS basado en plataforma TSP e interfaces

9.3.3. MTAS

Es un servidor de servicios SIP que forma el nivel de aplicación de la red multimedia y proporciona servicios básicos y avanzados de comunicaciones. El MTAS está compuesto por varios subelementos, un modulo de control, un módulo de gestión de información de suscriptor, un modulo de facturación, un modulo de operación y mantenimiento, un modulo de medios un modulo XDMS que asisten al funcionamiento del conjunto de servicios del servidor. Está implementado sobre el TSP 6.0 que utiliza tanto NSP 6.0 como NSP 5.0.

9.3.3.1. Estructura de control y servicio

Estructura de control que maneja la comunicación SIP con el CSCF actuando como un B2BUA. Es también el responsable de la comunicación con los servicios o aplicaciones residentes en el servidor.

9.3.3.2. Modulo de gestión de información de suscriptor

Modulo que obtiene, almacena en memoria y gestiona la información de suscriptores. Esta información almacenada en el HSS es descargada por este modulo y almacenada para las operaciones de los servicios. Afecta tanto a la información propia del perfil del suscriptor como la información relativa al servicio.

9.3.3.3. Modulo de XDMS

Modulo encargado de gestionar configuración de suscriptores relativos a servicios basados en formatos XML

9.3.3.4. Función de recursos de medios MRFC

Entidad definida como parte del servidor de aplicación MTAS y permite que el acceso y la selección de los medios de la red multimedia necesarios para la ejecución de las aplicaciones del servidor. Controla los medios de la red IP (MRFP) a través del protocolo de comunicación H.248 sobre la interfaz estandarizada Mp interactuando con las funcionalidades de procesamiento de flujos multimedia (mezcla de flujos de datos de uno o varios medios, transcodificación de los paquetes recibidos, cancelación de ecos, adaptación de velocidades de transmisión, etc..)

En la siguiente figura mostramos como es la implementación del MTAS y de todos sus módulos internos.

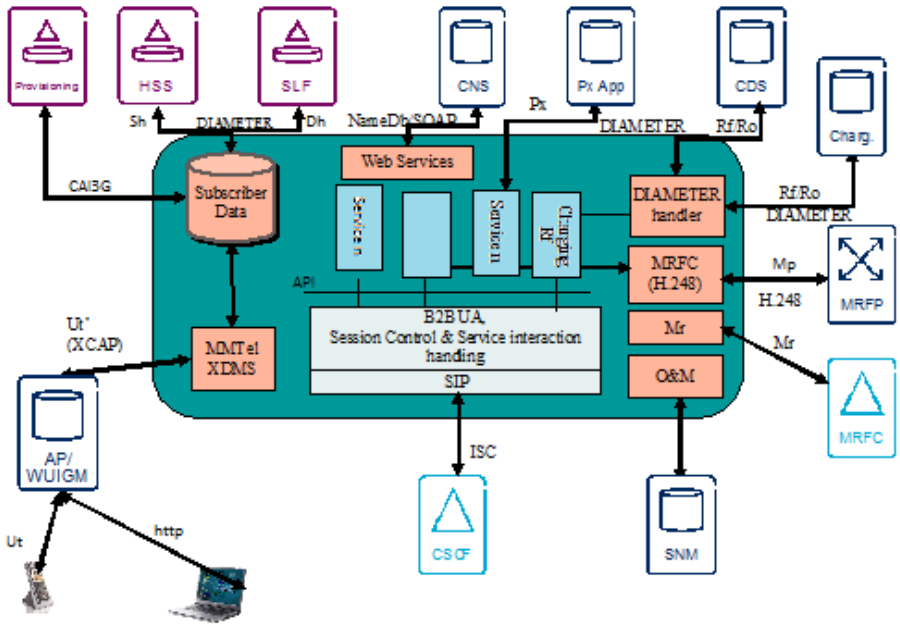

Figura 90. Arquitectura interna MTAS

9.3.4. Funciones de asistencia IP

Es el conjunto de funciones auxiliares que son necesarias para permitir el funcionamiento de una red IP. En la solución proporcionada para Orange se trata fundamentalmente de varias características.

Servidores DNS y ENUM, entidades fundamentales en el mundo IP para la resolución de nombres de dominios en direcciones de red y la resolución de numeración internacional E.164 y su traducción en direcciones SIP URI si procede.

Un servidor de DHCP para la asignación dinámica de direcciones de red para los usuarios y un servidor AAA para las funciones de seguridad de autenticación, autorización y registro de operaciones en la red.

Para la gestión y control de estas mismas funciones se despliegan paralelamente un sistema propio de configuración y mantenimiento. Todas estas operaciones pueden ser implementadas en nodos de red separados o en un nodo integrado.

9.3.5. SBC

Función implementada en redes IP que tiene como objetivo el control de todo flujo de datos entre redes de operadores de servicio que realiza múltiples tareas fundamentales de seguridad, control acceso, política de red, filtrado de tráfico y otras muchas más. Implementado por el equipo de la compañía ACME Packet Session Director 4500 proporciona todas las capacidades necesarias para el intercambio entre redes IP adyacentes.

9.3.6. Integración con el nivel de provisión

La solución MMTel 11A se integra junto con un sistema dedicado de provisión de usuarios y servicios para éstos denominado sistema de Multi-Activación de Ericsson o EMA, que proporciona una interfaz única para la provisión y la gestión integral y centralizada de todos los servicios que cada usuario tiene suscritos.

El EMA puede provisionar diferentes tipos de servicios:

- Servicio básico de provisión

  Registra y almacena la información básica del usuario en los repositorios de información de la red (HSS, SLF, ENUM Server, etc.)y permite que el usuario acceda a los servicios de la red.

- Servicio básico de telefonía multimedia

  Provisiona y habilita un usuario en un servidor de telefonía multimedia MTAS para que pueda acceder a los servicios habilitados en este. Modifica también el perfil de usuario en el HSS.

- Servicios multimedia

  Provisiona uno o varios servicios multimedia ofrecidos por un MTAS en el perfil de un usuario dado. Representa los servicios a los que está suscrito un usuario en un momento dado.

El EMA se conecta directamente con el repositorio de datos de clientes (HSS), los servidores de aplicación MTAS y sobre algunas funciones auxiliares como los DNS y ENUM y por otro lado por medio de con el subsistema de administración de clientes de Orange. La siguiente figura muestra la interacción:

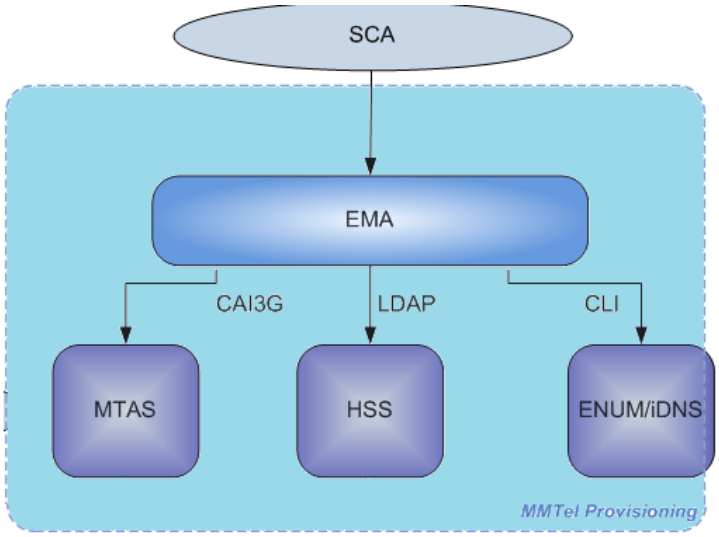

Figura 91. Integración de plataforma de provisión MMTel en la red de Orange

Por requerimiento de Orange es necesario que la herramienta de administración de clientes de Orange SCA se integre con el EMA. En el escenario actual el SCA directamente interactuaba con cada nodo de red por medio de peticiones SOAP/HTTP de una forma muy poco eficiente. En el escenario que se quiere implementar el SCA en lugar de atacar a cada nodo de red se comunicará únicamente con el EMA y este adaptará por medio de una personalización las peticiones SOAP/HTTP del SCA a las ordenes de la lógica interna CAI3G del EMA.

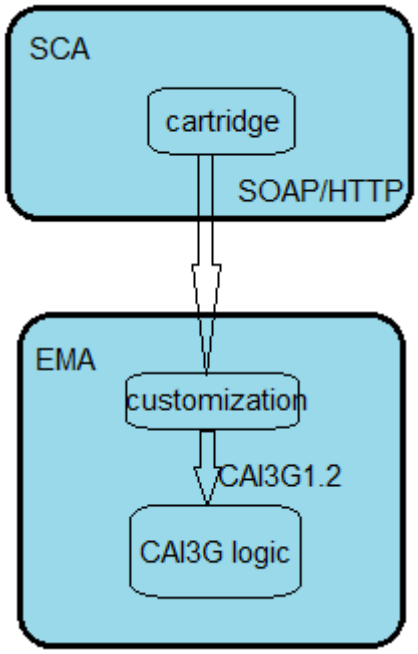

Figura 92. Interfaz de integración plataforma EMA en plataforma de provisión SCA actual.

9.3.7. Sistema de tarificación

El sistema de de multimedia de Ericsson en su última versión proporciona el sistema de tarificación offline o diferido para el IMS. Este sistema realiza las funciones propias de estos subsistemas como describimos en el punto 4.8.3.

Toda la actividad de los usuarios en la red genera información de tarificación y facturación, en el nivel de aplicación MTAS y en el nivel de control S-CSCF, en forma de evento de facturables. Esta información es recolectada por una función interna del sistema de Multi-Mediación denominada DEC que es la implementación realizada por Ericsson de la función CDF del punto 4.8.3.2. Una vez que los eventos han sido recolectados por esta función son preprocesados, filtrados y almacenados en ficheros ASCII y finalmente retransmitidos en intervalos de tiempo pequeños al servidor de multi-mediación. Este sistema es la ejecución de la función CGF de Ericsson descrita en el punto 4.8.3.3. En el instante en que esos ficheros están presentes en este servidor, son leídos y organizados (separados por tipo de servicio, nodo generador, etc.).Posteriormente es procesados por según la lógica oportuna para cada tipo de ficheros y formateado y consolidados dando como resultado final la generación de registros de salida o CDR que son almacenados y reenviados al sistema de facturación de Orange, denominado Platine. La siguiente figura ilustra la arquitectura explicada.

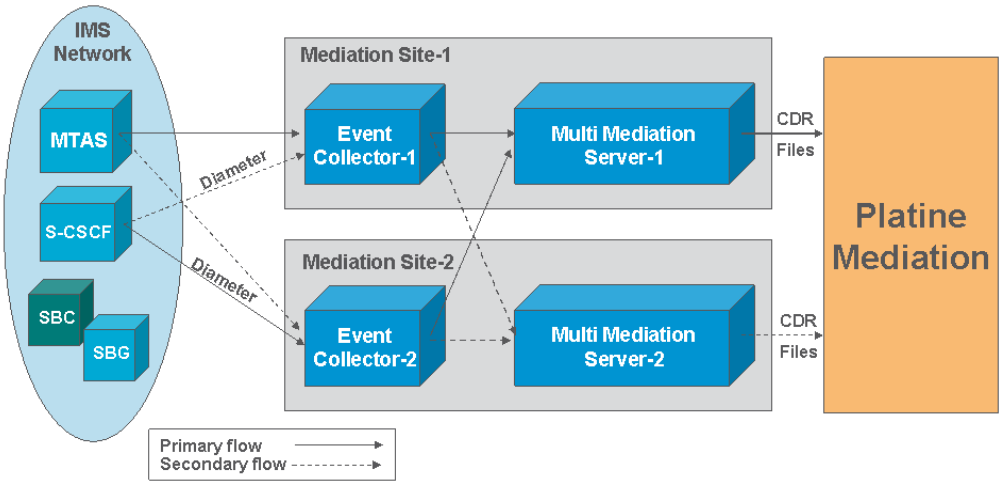

Figura 93. Despliegue plataforma de multimediación en red IMS

En esta arquitectura tanto el DEC como el servidor de Multi-Mediación son desplegados en un mínimo de dos localizaciones con una configuración de redundancia primario-secundario o activo-espera. Los nodos de red envían los eventos tarificables al DEC definido como primario o activo si esta operativo y sin averías y al secundario-espera en caso de caída del primer DEC. El DEC a su vez retransmite los ficheros recibidos de la misma forma. El despliegue inicial se realizará en las localizaciones Coslada y Ulises.

El protocolo de transferencia de ficheros utilizado entre el DEC y el servidor de MM y éste y el sistema de facturación exterior, es el protocolo seguro de transferencia de ficheros SFTP.

9.3.7.1. Implementación hardware

El sistema de multi-mediación para la red IMS será la versión 7.1. Este sistema hace uso de de servidores SunMicrosystems x86 basados en arquitectura blade. El modelo concreto es el Sun Bladex6270M2. Cada servidor blade tiene:

- 2 unidades de procesamiento con 4 núcleos cada una.
- 48 GBytes de memoria RAM
- 4 discos duros internos de 146 GBytes cada uno
- 6 puertos de comunicación Gigabit Ethernet
- 2 canales para conexiones de fibra óptica.

Los servidores blade pueden ser montados en chasis propios que permiten importantes ahorros de espacio, consumo de energía y costes comparados con los servidores convencionales. El chasis SB 6000 permite la integración y la expansión de hasta 10 servidores blade.

Adicionalmente se puede desplegar una cabina de discos EMC2 para ofrecer capacidades de almacenamiento. El modelo seleccionado es un EMC AX4-5 equipado con 12 discos de 300 GB cada uno y expandible hasta los 60 discos.

El despliegue inicial se realizará en las ubicaciones de Coslada y Ulises con la siguiente configuración:

- 1 chasis SB 6000
- 2 servidores blade SUN X6270M2
- 1 cabina de discos EMC AX4-5

9.3.7.2. Implementación software

La versión software 7.1 es una arquitectura multiproceso y multitarea que permite a los usuarios manejar de una forma sencilla la plataforma. El servidor DEC será la aplicación de MM con funcionalidades limitadas mientras que para el servidor MM se incluye la aplicación con las funcionalidades completas.

9.3.8. Sistema de gestión y supervisión de errores

Ericsson proporciona un sistema de supervisión y monitorización centralizado de alarmas generadas en los elementos de red del subsistema multimedia. Esta plataforma denominada OSS-RC recolecta todas las alarmas e información de errores generada por cada nodo de la red y los clasifica, identifica y ordena en función de su criticidad e impacto en cada función.

Este subsistema está a su vez conectado a su vez con el subsistema de supervisión de alarmas NMS de Orange (plataforma IBM Netcool) y los nodos de la red IMS por medio de CORBA.

El subsistema está basado en la supervisión y monitorización de diferentes nodos de la red:

- Entidades de servicio. Los errores pueden ser de la propia plataforma TSP (CSCFs, HSSs, MTASs, etc.). Es decir generado por un nodo de la plataforma, debido a problemas físicos, de configuración o de servicio. Estos errores son gestionados a través del modulo de gestión de errores de la plataforma de servicio (TSP FM).
- Entidades de red, como los servidores DNS, ENUM, DHCP, SBC etc. Estos nodos hacen la gestión de eventos, errores y alarmas por medio de clientes SNMP internos que envían mensajes a un servidos SNMP que recibe todas las alarmas de estos elementos de red. El servidor SNMP es el que enviará los mensajes de alarma al gestor de alarmas de la red OSS-RC.
- Entidades de medios. Un gestor de alarmas y errores que controla la función de medios y por lo tanto el estado y la disponibilidad de todos los medios y funciones de gestión de los medios existentes.

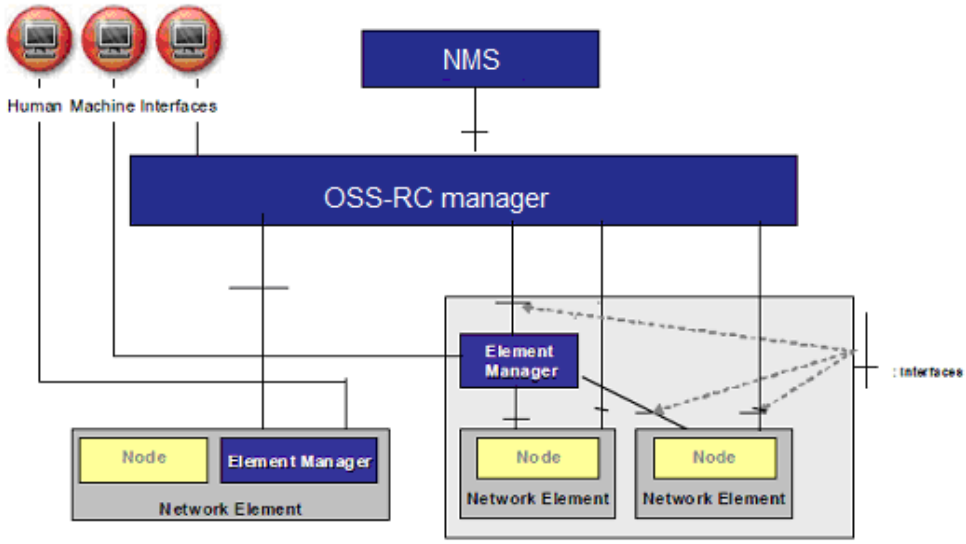

Figura 94. Arquitectura interna sistema de mantenimiento, monitorización y supervisión.

La solución OSS-RC 11.2 está desplegada sobre varios servidores SUN localizados en el emplazamiento de Coslada o Meneses.

9.3.9. Conectividad IP

Ericsson dispone de una solución para proporcionar la conectividad IP indispensable dentro de la arquitectura multimedia y de esta con el resto de la red

del cliente. El conjunto de elementos de routers, firewalls, switches y puesta de seguridad (SBCs) desplegados dentro del nivel de red del IMS forma el denominado MPBN, o red troncal de conectividad de paquetes que permiten asegurar la conectividad IP entre nodos, servidores y equipos de acceso e interconexión.

La infraestructura propuesta tiene como objetivo proporcionar a la red características de alta disponibilidad, escalabilidad, seguridad y modularidad que aseguren la integración del dominio multimedia y la migración de usuarios al nuevo dominio.

9.3.9.1. Conectividad intra IMS

Para la conectividad entre entidades o nodos desplegados en un mismo despliegue IMS Ericsson propone el uso de la plataforma SmartEdge 600 que proporciona todas las funciones de conectividad IP dentro de un despliegue multimedia y hacia el exterior del despliegue. Estos routers de alta disponibilidad y ampliamente probados en redes reales consisten en una estructura modular formada por un chasis, procesadores de conexión cruzada, interfaces, transceptores y software. Estas estructura se puede es fácilmente escalables pues permite la inserción de hasta 8 módulos con 2 ranuras para redundancia de los procesadores de ruta en forma 1:1. Estos routers incorporan una tarjeta ASE que proporciona comunicaciones IPsec hacia el exterior del emplazamiento. En la configuración actual de las 6 ranuras restantes el chasis mantiene 3 ranuras disponibles para futura ampliaciones de capacidad de conmutación y enrutamiento. La figura 94 muestra las entidades desplegadas por emplazamiento.

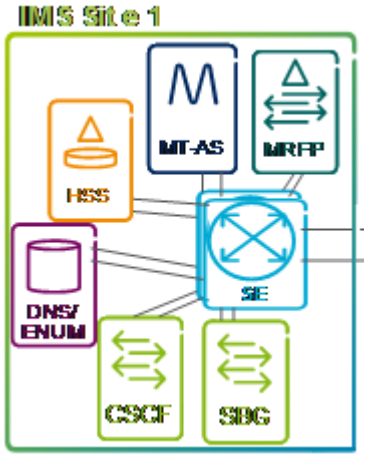

Figura 95. Configuración en emplazamiento de funciones core de IMS

9.3.9.2. Conectividad con elementos externos

Para la interconexión de las redes de dos proveedores de servicio se emplean además de las soluciones en el nivel de control y transporte MSS explicados en el capítulo 8, en el nivel de conectividad IP un grupo de routers de interconexión que proporcionan las funciones de seguridad y aislamiento de tráfico requeridos entre dominios diferentes.

También proporcionan conectividad con las redes de acceso del operador interconectándose con otros elementos sobre el backbone IP de Orange.

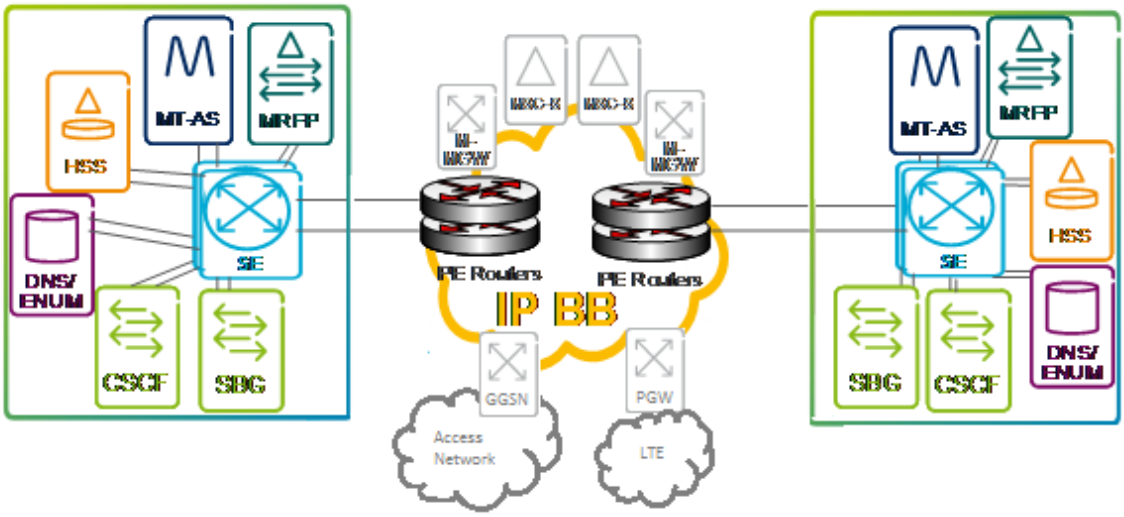

Figura 96. Comunicación e interconexión a nivel de red de emplazamientos core IMS y red de transporte IP

Los routers PE y SE se comunican por medios de 10 puertos GigaEthernet de interconexión física. El principal método de conexión entre entidades que pertenecen a dominios distintos es por medio de conexiones VPN sobre la red troncal IP (backbone).

9.3.10. Seguridad

La seguridad es una característica principal en el despliegue de IMS y en la migración de usuarios al dominio multimedia. La seguridad está presente tanto en los nodos de la red como en el dominio en su conjunto. Para implementar las funciones de seguridad Ericsson parte de las especificación del seguridad de IMS explicadas en el capitulo 3.2.4.

9.3.10.1. Seguridad de acceso

Se encarga de las funciones de seguridad entre el terminal del usuario y la red IMS (conexión SIP, conexiones Web o conexiones XCAP entre otras) según se explica en el punto 3.2.4.4. Con respecto a la securización de la conexión SIP el método principal para usuarios

móviles basados en tarjetas inteligentes USIM/ISIM, es el uso del protocolo IMS-AKA. Para el conjunto de terminales de móviles que nos soporte el mecanismo IMS-AKA se utilizan los mecanismos de seguridad GIBA del punto 3.2.4.5.3, para redes de acceso securizadas el método del punto 3.2.4.5.4, y finalmente para el resto de terminales de usuarios que no pertenecen al dominio móvil a través de SIP Digest y de NASS-IMS.

9.3.10.2. Seguridad en el dominio multimedia.

Ericsson implementa los conceptos de seguridad para el dominio multimedia del punto 3.2.4.3. Establece un principio de "defensa en profundidad" en base a diferentes niveles de seguridad dentro del dominio estableciendo un perímetro de seguridad, protección interna entre elementos desplegado en un mismo emplazamiento y protección de nodo o entidad.

El primer nivel de defensa es por tanto el perímetro de seguridad que está compuesto por los routers SE del emplazamiento, los firewall que proporcionan las funcionalidades de filtrado y acceso y las puertas de acceso de seguridad o SBCs para las redes de acceso cableadas y las interfaces entre diferentes redes junto con los router PE de interconexión. Para las redes de acceso móvil también el PCRF/P-CSCF realiza parcialmente funciones de SBC.

La segunda línea de protección consiste en la protección de la comunicación entre nodos de un mismo emplazamiento por medio de la segmentación del tráfico por medio de VLANs. A su vez se protege el trafico de salida del router SE hacia el router PE securizando las comunicaciones por medio de IPsec.

Finalmente la protección intra-nodo que consiste en la protección física de acceso a cada nodo y las herramientas de seguridad y control de puertos, software y aplicaciones instaladas en el nodo (node hardening).

9.3.10.3. Seguridad en el dominio de mantenimiento y operación (O&M)

La securización del nivel de operación y mantenimiento es especialmente sensible puesto que a través de este nivel se pueden producir cambios en las configuraciones de los nodos de IMS o del backbone. Esto se consigue en primer lugar separando el subsistema de O&M de los dominios de la red multimedia (de medios y de control) estableciendo para este como un dominio de seguridad a parte.

El dominio de O&M también se segmenta creando a su vez cuatro dominios de seguridad (infraestructura multimedia, red corporativa, facturación y servicios OSS) que son interconectados entre sí por medio de un router con funcionalidad firewall que controla toda la comunicación entre dominios. Dentro de cada dominio de seguridad el flujo de tráfico no está controlado. El router también realiza funciones de segmentación entre los distintos dominios.

Adicionalmente se establece una política de privilegios de acceso a la plataforma O&M en base a un conjunto de perfiles de acceso y usuarios definidos en el sistema para controlar que operadores acceden a la plataforma, en qué condiciones y con qué permisos. Los dominios definidos dentro de la plataforma de O&M.

9.4. Despliegue de la arquitectura

Por requerimiento de disponibilidad y fiabilidad la solución será desplegada en una configuración de redundancia geográfica con una primera instalación de dos emplazamientos físicos cada uno de los cuales albergará los mismos nodos /entidades de red. La configuración de operación entre los dos emplazamientos estará basada en el modelo de redundancia 1+1, primario/secundario o activo/reserva o espera. Esto significa que el emplazamiento configurado como primario o activo para un usuario proporcionara el servicio bajo condiciones normales y el emplazamiento definido como secundario solo entrara en juego en caso de fallo o caída de servicio del primario. Bajo este modelo cada uno de los despliegues realizados tiene que ser proporcionadamente dimensionado para que sea capaz de soporta el 100% del tráfico de la red en caso de pérdida de servicio del otro emplazamiento.

Sin embargo para la optimización de uso de los recursos y facilitar el traspaso de servicios en caso de caída de uno de los nodos/emplazamientos, algunas funciones o entidades son configuradas bajo distribución o balanceo de carga de servicio, esto quiere decir que cada emplazamiento estará configurado como emplazamiento primario o activo para el 50 % de los usuarios de la red y como secundario o en reserva para el otro 50 % de los usuarios y viceversa. Esta configuración permite que en caso de fallo el nodo asuma el otro 50% de usuario que tenían configurados a este como secundario. Este modelo de distribución de carga es configurado para los nodos CSCF (E-CSCF, I-CSCF, P-CSCF, S-CSCF) SBG (SBC) DNS, MSS (MGCF, M-MGW) y MTAS. Este modelo de distribución provoca que en caso de caída de un nodo o un emplazamiento los datos de facturación y de sesiones activas se pierdan (warm-standby) y en algunos nodos también los datos del registro de usuario en la red (cold-standby) forzando el re-registro del terminal de usuario.

El único elemento del emplazamiento que nos soporta esta configuración de balanceo de carga será el HSS/SLF donde el nodo HSS configurado como primario o activo lo será para el 100% de los usuarios, permaneciendo el otro como espera. Las entidades HSS/SLF es recomendable que sean integradas en un mismo nodo y configuradas en el modo activo/espera explicado.

En función de si los datos tienen que ser replicados entre los nodos configurados como activos y los nodos configurados como pasivos o en espera al mismo tiempo (hot-standby) con pequeña diferencias de tiempo entre el activo y el de reserva (warm-standby) o con grandes diferencias de tiempo (cold-standby) se completa el modo de operación de los diferentes nodos.

A parte de esta consideración es también importante que en ambos emplazamientos los suscriptores estén idénticamente provisionados (hot-standby).

9.4.1. Redundancia

Los elementos principales de la red troncal (CSCF, HSS) se despliegan sobre la plataforma TSP como se ha indicado, que es la que proporciona las características de alta disponibilidad y redundancia de los nodos. Esta plataforma se basa en el concepto de duplicidad de las mayor parte de los módulos físicos que integra (, procesadores, módulos de memoria, fuentes de alimentación, tarjetas físicas para propósitos distintos, interfaces de comunicación propias para la plataforma O&M separadas de las plataformas de tráfico, etc.) y lógicas (configuración de interfaces virtuales en las tarjetas de comunicaciones, etc.) Los MTAS que también se implementan por medios de las plataformas TSP se configuran a diferencia del resto de nodos en cluster en modo N+1 permitiendo que la selección de servidor de aplicación se haga de forma dinámica en función de la disponibilidad, carga y estado de cada servidor y en caso de caída de un MTAS lo usuario de dicho servidor son traspasado a otro MTAS del cluster.

Las funciones MRFP se basan en clusteres de servidores HP Proliant DL 380 que proporciona las capacidades de procesamiento y la interfaz de comunicación H.248 con la función MFRC y un conjunto de servidores de medios. Cada clúster MRFP está configurado en redundancia N+1 y en caso de caída de uno de los servidores de procesamiento o de uno de los servidores de medio otro servidor asume la carga del servidor afectado. Cada clúster proporciona capacidades a un MRFC (implementado en el MTAS) de forma simultánea pero puede servir a varios MRFC de forma no simultánea.

Para los SBC entre dominios se despliegan en pares conectados entre ellos por medios de dos puertos de gestión que permite configurarlos en modo activo/espera de forma que entre ambos comportan información de estado, disponibilidad, uso, configuración, etc. para en caso de fallo de uno de ellos el otro elemento sea capaz de tomar el control sin interrupción de servicio.

Para la plataforma de provisión EMA se emplea una configuración de multi-nodo independientes configurados en balanceo de carga que proporciona un sistema de muy alta disponibilidad.

La plataforma de gestión y mantenimiento OSS-RC consiste en un conjunto de servidores conectados a una cabina de discos redundados configurados en espejo en tiempo real donde se crean dos copias de datos en paralelo a la misma vez para que la caída de un disco o de una unidad no provoque la perdida de la gestión de la red.

9.4.2. Escalabilidad

9.4.2.1. MTAS, CSCF y HSS

La implementación física de elemento de red basado en las arquitecturas blade permite que en caso de necesitar incrementar el número de equipos físicos para la red multimedia esto se haga fácilmente a través de la ampliación de servidores blade que son insertados en chasis

multi servidores que cubren todas las necesidades para el despliegue de estos.

9.4.2.2. Elementos de red DNS

Los elementos de funciones de red se escalan de acuerdo a principio tradicionales como en el caso de los servidores DNS que actúan de forma independiente y no sincronizada dentro de la red. La forma de escalarlos es directamente mejorando los recursos internos de cada servidor (memoria, capacidad de procesamiento, etc.) o desplegando nuevos servidores en la red más potentes.

9.4.2.3. ACME SBC

El equipamiento desplegado soporta hasta 32000 sesiones simultaneas, 200000 túneles IPsec, tablas de routing de hasta 2 millones de registros, la transmisión de hasta 16000 mensajes DIAMETER por segundo, interfaces de red 1000/100/10M Ethernet.

9.4.2.4. EMA

El despliegue puede realizarse en base a diferentes volúmenes de suscripciones:

- Un servidor de baja capacidad para hasta 500000 suscripciones.
- Un servidor de media capacidad para dos millones de suscripciones.
- y una configuración de dos servidores en alta disponibilidad para hasta cuatro millones de suscripciones.

9.4.2.5. MM

Un chasis blade con capacidad de hasta 10 servidores blade y la posibilidad de colocar una cabina con dos chasis para 20 servidores blade adicionales y con una cabina de discos de hasta 60 unidades de 300 GB para un total de 17,5 TB.

9.4.3. Escenario de despliegue de IMS

9.4.3.1. Despliegue inicial

Para el soporte de hasta 500000 suscripciones MMTel se despliegan en cada uno de los dos emplazamientos originales 3 racks con la siguiente distribución:

- Primer rack. Con tres chasis TSP para las funciones de CSCF (S-CSCF, P-CSCF, I-CSCF, E-CSCF) HSS y MTAS.
- Un segundo rack con 4 clústeres de ACME SBC Sesion Director 4500 (cada cluster compuesto por 2 servidores)
- Un tercer rack con dos servidores HP ProLiant DL 380 G6 para las capacidades de procesamiento de las funciones DNS/ENUM y un servidor del mismo tipo de almacenamiento de datos. No se instala cabina de discos.
  Dos servidores HP Proliant DL 380 G7 para las funciones MRFP y dos routers SmartEdge 600.

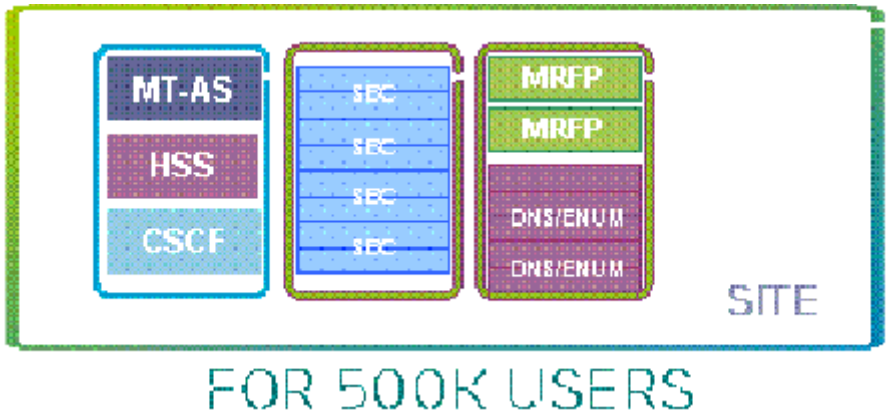

Figura 97. Instalación de servidores y racks por emplazamiento IMS para la 1ª fase

9.4.3.2. 2ª fase de despliegue

Para el soporte de un millón de suscripciones se desplegará un nuevo rack con dos chasis blade TSP para funciones adicionales CSCF y MTAS

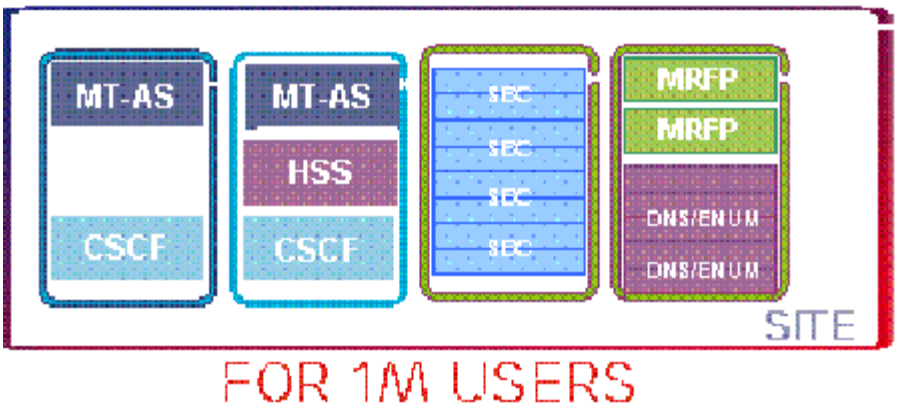

Figura 98. Instalación de servidores y racks por emplazamiento IMS para la 2ª fase

9.4.3.3. 3ª fase de despliegue

Para el soporte de 1290000 suscripciones serán necesario añadir un nuevo chasis blade TSP para un nodo HSS. Además del este despliegue físico serán necesario actualizar las licencias de todos los nodos implementados en las fases anteriores y que están limitados a un millón de suscripciones.

9.4.3.4. Nodo de MM

El despliegue inicial esta realizado en base a servidores hardware que soportan sobradamente los niveles de despliegue de las 3 fases y solo requerirán actualizaciones de licencias de uso.

9.4.3.5. EMA

El despliegue de la solución de provisión se realizara en dos emplazamientos geográficos redundados que permitirán la provisión de suscripciones de usuarios y servicios en ambos emplazamientos IMS

9.4.3.6. OSS-RC

El despliegue de una red de supervisión y monitorización para el dominio multimedia será necesario para la primera fase y estará compuesto por herramientas de gestión de caídas y errores, configuración O&M y soporte de operaciones. Para posteriores fases de despliegue hasta la fase 3ª no será necesario la ampliación de hardware pero si de licencias de uso.

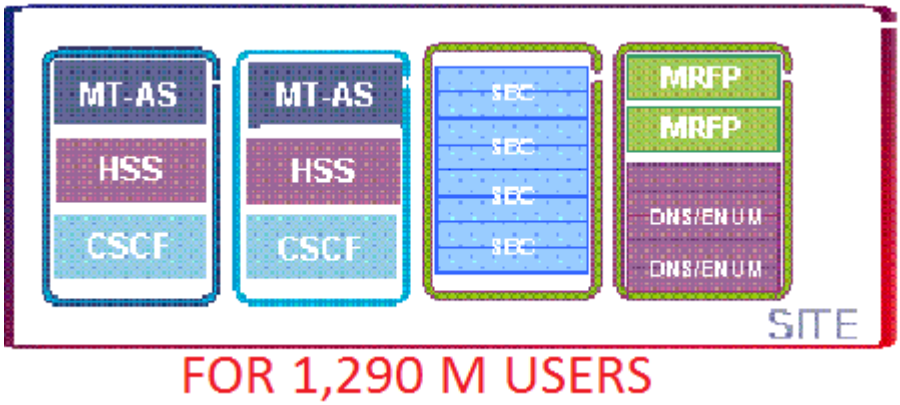

Figura 99. Instalación de servidores y racks por emplazamiento IMS para la 3ª fase

9.5. Migración e interconexión de dominios

El despliegue y la migración de usuarios tendrá lugar a través de 3 fases, un piloto de pruebas basado en la migración de 2000 usuarios de Orange de banda ancha fija (ADSL), una fase de transferencia de trafico de VoIP de la solución de NokiaSiemens actual a la red troncal multimedia de Ericsson.

9.5.1. 1ª Fase

Fase de piloto de pruebas con 2000 usuarios. Iniciada en Diciembre de 2011. El tráfico de estos dos usuarios tiene que ser conmutado de las redes de acceso hacia los MSS (MSC-S/MGCF y M-MGW) sin redundancia de los emplazamientos de Coslada y Ulises. El establecimiento de 5 E1 de capacidad por emplazamiento permitirá la gestión de 99 Erlangs de tráfico (unidad de medida que indica que se usan 99 canales o conexiones por hora) con una carga de uso de 40%.

9.5.2. 2ª Fase o fase de traspaso

Dividido en 2 pasos:

Un primer paso correspondiente (Enero 2012) a la migración de trafico de la plataforma de IMS actual a la plataforma IMS de Ericsson enrutando el trafico de 450000 usuarios hacia los MSS de Coslada y Ulises (sin redundancia) que proporcionaran 22275 Erlang o canales/conexiones por hora con un total de 930 E1 de capacidad y un uso del 80 %.

Un segundo paso (Febrero 2012) con la introducción de redundancia de emplazamiento introduciendo un emplazamiento más de M-MGWs resultando en una configuración de sitio 2+1 con volúmenes y parámetros similares al paso primero.

9.5.3. 3ª fase o fase de distribución

La migración de hasta un millón de usuarios en dos pasos finales (Mayo y Diciembre 2012) con 49500 conexiones/canales ocupados por hora y hasta 2408 E1 de capacidad (un 2,5 G aprox.).En el primer paso se distribuirá el tráfico en hasta 7 emplazamiento de M-MGWs en dos áreas y el segundo paso incluyendo un área adicional.

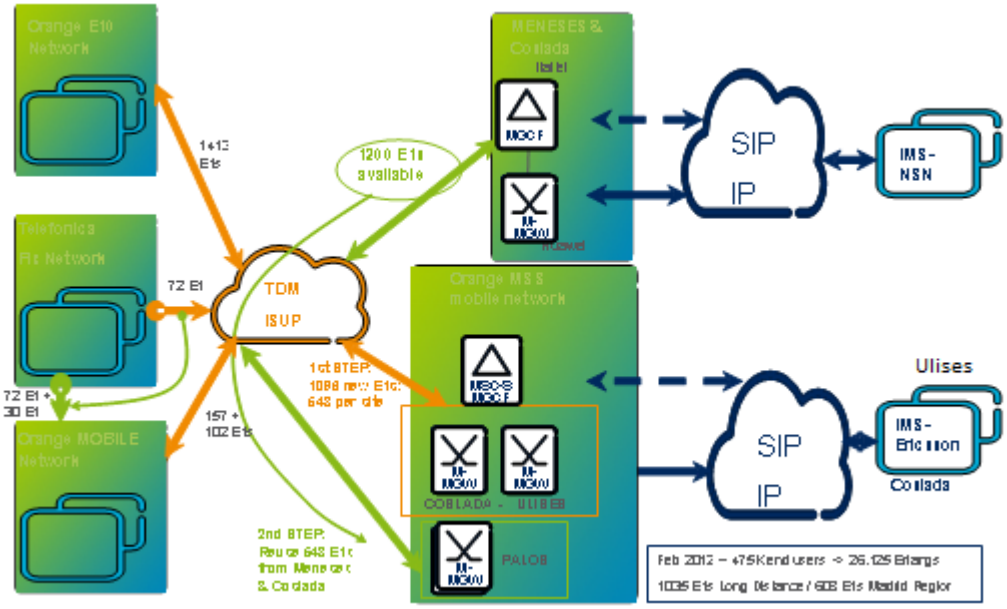

Figura 100. Diagrama de fase de migración de usuarios a Ericsson IMS

Conclusiones

10. Conclusiones

Como resumen a todo lo expuesto en el anterior trabajo, en un primer punto se han introducido de forma breve la evolución y transformación del núcleo de red en redes móviles desde su aparición hasta hoy en día y como se ha ido cambiando el principio de arquitecturas verticales de servicios donde cada servicio es proporcionado por una infraestructura diferencia del resto dando lugar a la existencia de redes de comunicaciones superpuestas.

En la segunda parte del estudio (capítulo 2- 6) se introdujeron y detallaron los conceptos de redes de nueva generación desarrollados durante la última década por las organizaciones de estandarización y que están en continua en evolución (Release 11) centrándonos fundamentalmente en la evolución y desarrollo de un núcleo de red completamente IP (IMS) que facilita la transformación definitiva de las redes de comunicaciones móviles en redes de comunicaciones multimedia horizontales multiservicio y multiacceso y que preparan y actualizan éstas para la llegada de la 4ª Generación de comunicaciones móviles digitales que completarán la transformación en redes 100% IP.

Finalmente una tercera y última parte de estudio, detalla cuales son las circunstancias y los enfoques que se plantean dentro de la industria para implementar redes de nueva generación y nos centramos en el caso práctico que está teniendo lugar para la interconexión e integración de una solución multimedia desarrollada por Ericsson AB para la red comercial del operador Orange España, que tiene como objetivo final facilitar el desarrollo de nuevos modelos de negocio a los operadores de red que permitan a estos encarar los nuevos retos y oportunidades de un mundo donde cada día las personas tiene un estilo de vida más digital y donde las comunicaciones constituyen un elemento principal de la vida de las personas.

Acrónimos

3DES	Triple Data Encryption Standard
3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
64QAM	64 bits Quadrature Amplitude Modulation
AAA	Authentication, Authorization & Accounting
AAL2	ATM Adaptation Layer 2
ABMF	Account Balance Management Function
AKA	Authentication Key Agreement
AMR	Adaptive Multi-Rate audio codec
API	Application Programming Interface
AS	Application server
ASCII	American Standard Code for Information Interchange
ATM	AsincronousTransfered Mode
AuC	Authentication Center
AUTN	Authentiction number
AXE	Automatic Cross-Connection Equipment
BCF	Break In Control Function
BGCF	Breakout Gateway Control Function
BICC	Bearer Independent Call Control
BSC	Base Station Controller
BSS	Business Supoort Subsystem
BTS	Base Transceiver Station
CA	Certification Authority
CAMEL	Customised Application Mobile Enhanced Logic
CAMEL SE	CAMEL Service Environment
CAMEL SSF	CAMEL Service Switching Function
CCU	Control Channel Unit
CDF	Charging Data Function
CDMA	Code Division Multiple Access
CDR	Call Duration Record
CEPT	Conference Europeenne des Administrations des Postes et des Telecommunications
CGF	Charging Gateway Function
CK	Ciphenring Key
CORBA	Common Object Request Broker Architecture
CP	Central Processor
CS	Circuit Switched
CSCF	Call Session Control Function
CS-MGW	Circuit-Switched Media Gateway
CTF	Charging Trigger Function
DEC	Distributed Event Collector
DHCP	Dinamic Host Control Protocol
DNS	Domain Name Server
DTMF	Dual Tone Multi-Frecuency
EBCF	Event Based Charging Function
E-CSCF	Emergency Call Session Control Function

EDGE	Enhanced Data rates for Gsm Evolution
EGPRS	Evolved General Packet Radio Service
EIR	Equipment Identity Register
EIVP	Encapsulated ISUP Version Profile
E-NodeB	Evolved Node B
ENUM	E.164 NUmber Mapping
EPC	Evolved Packet Core
EPC-GW	EPC Gateway
EPS	Evolved Packet System
ESP	Encapsulation Security Payload
ETSI	European Telecommunication Standard Institute
E-UTRAN	Evolved UTRAN
FM	Fault Management
GCP	GAteway Control Protocol
GERAN	Gsm Edge Radio Access Network
GESB	Generic Ethernet Switch Board
GGSN	Gateway GPRS Support Node
GMSC	Gateway Mobile Switching Center
GPRS	General Packet Radio Service
GRUU	Globally Routable User Agent URI
GSM	Global System for Mobile communications
HDTV	High Definition Television
HLR	Home Location Register
HSDPA	High Speed Downlink Packet Access
HSPA+	High Speed Packet Access plus
HSS	Home Suscriber Server
HSUPA	High Speed Uplink Packet Access
IBCF	Interconnection Border Control Function
I-CSCF	Interrogating Call Session Control Function
IETF	Internet Engineering Task Force
iFC	Initial Filter Criteria
IK	Integrity Key
IKE	Internet Key Exchange
IM- GW	IP Multimedia Gateway
IMPI	IP Multimedia Private Identity
IMS	IP Multimedia Subsistem
IMS ALG	IMS Application Level Gateway
IMS CN	IMS Core Network
IMS GWF	IMS Gateway Function
IMT-Advanced	International Mobile Telecommunication- Advanced
IP	Internet Protocol
IP-CAN	IP conectivity access network
IPsec	IP secured
IPTV	Internet Protocol Television
IPv4	IP version 4
IPv6	IP version 6
ISC	IP Service Control
ISDN	Integrated Services Digital Network
ISIM	IMS SIM
ISUP	ISDN User Part

ITU	International Telecommunications Union
ITU-R	ITU-Radiocommunications
IVR	Interactive Voice Response
K	Shared Key
LRF	Location Retrieval Function
LTE	Long Term Evolution
M3UA	MTP Level 3 (M3) User Adaptation
MAC	Media Access Control
MD5	Message-Digest Algorithm 5
MEGACO	Media Gateway Control
MGCF	Media Gateway Control Function
MIMO	Multiple Input Multiple Output
MME	Mobility Management Entity
M-MGW	Mobile Media Gateway
MMTel	MultiMedia Telephony services
MPBN	Mobile Packet Backbone Network
MRB	Multimedia Resource Broker
MRF	Multimedia Resource Function
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
MSC	Mobile Switching Center
MSC-S	MSC Server
MSS	Mobile Softswithing Solution
MTAS	Multimedia Telephony Application Server
MTP	Message Transfer Part
NAPT	Network Address Port Translation
NAPT-PT	NAPT-Protocol Translation
NASS	Network Attachment SubSystem
NAT	Network Address Translation
NDS	Network Domain Security
NMS	Network Management Subsystem
NSP	Network ServerPlatform
O&M	Operation & Management
OCF	Online Charging Function
OCS	Online Charging System
OFCS	Offline Charging System
OFDM	Orthogonal Frecuency Division Multiplex
OSA	Open Service Architecture
OSA SCS	OSA Service Capabilities Server
OSS	Operation Support Subsystem
OSS-RC	Operation Support System - Radio and Core network
PCC	Policy & Charging Control
PCEF	Policy & charging enforcement Function
PCM	Pulse Code Modulation
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy Call Session Control Function
PDG	Packet Data Gateway
PDN	Packet Data Network
PDN-GW	Packet Data Networks Gatwway
PDU	Packet Data Unit

PLMN	Public Land Mobile Network
PSI	Public Service Identifier
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAND	Random number
RES	Response
RF	Rating Function
RNC	Radio Network Controller
RSI	Route Set Information
RTP	Real Time Protocol
SA	Security Association
SBC	Session Borde Controller
SBCF	Session Based Charging Function
SCI	SIP trunk Configuration Information
S-CSCF	Serving Call Session Control Function
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SEG	Security Gateway
SGSN	Serving GPRS Support Node
SGW	Signalling Gateway
S-GW	Serving Gateway
SHA-1	Secure Hash Algorithm - 1
SigComp	Signalling Compression
SIGTRAN	Signalling Transport
SIM	Suscriber Identity Module
SIP	Session Initiation Protocol
SIP URI	SIP Uniform Resource Identifier
SLA	Service Level Agreement
SLF	Suscription Locator Function
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SQN	Sequence Number
SS7	Signalling System 7
TCP	Transmission Control Protocol
TEL URL	Telephone Uniform Resource Locator
TFO	Tandem Free Operation
THIG	Topology Hiding Inter-network Gateway
TISPAN	Telecomunications and Internet converged Services and Protocol for Advanced Networking
TLS	Transport Layer Security
TrFO	Transcoder Free Operation
TrGW	Transition Gateway
TSP	Telecom service Platform
UDP	User Datagram Protocol
UE	User Equipment
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
URN	Uniform Resource Name
USIM	UMTS SIM

UTRAN	Universal Terrestrial Radio Access Network
VCC	Voice Call Continuity
VLAN	Virtual Local Area Network
VLR	Visitor Location Register
WAG	WLAN Access Gateway
WCDMA	Wideband Code Division Multiple Access
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
XDMS	XML Document Management Service
XMAC	eXpected MAC
XRES	eXpected Response

Tabla de Figuras

Referencias Bibliográficas

[1] Gsm Switching, Services And Protocols 2º Edition (2001); Jörg Eberspächer, Hans-Jörg Vögel, Christian Bettstetter

[2] Las Telecomunicaciones y la Movilidad en la Sociedad de la Información por iniciativa de AHCIET; Edición: División de Relaciones Corporativas y Comunicación de Telefónica I+D.

[3] GSM Networks: Protocols, Terminology, and Implementation; Gunnar Heine, 1999 ARTECH HOUSE, INC.

[4] ITU Academy Portal Distance Learning on New Generation Network Management Approach. Semana_03_NGN_GET.pdf

[5]Comunicaciones Móviles Digitales. Transparencias de Comunicaciones móviles 3G: GPRS, departamento de Ingeniería Audiovisual y Comunicaciones, EUITT, Universidad Politécnica de Madrid.

[6]Comunicaciones Móviles Digitales. Transparencias de Comunicaciones móviles 3G: UMTS, departamento de Ingeniería Audiovisual y Comunicaciones, EUITT, Universidad Politécnica de Madrid.

[7] Redes móviles de tercera generación. Ángela Hernández. Departamento de Ingeniería electrónica y Comunicaciones. Universidad de Zaragoza.

[8] SAE/EPC.The core network of LTE. Gerhard Fritze M.Sc.Customer Solution Manager. Ericsson Austria GmbH/04/2008.

[9] Redes de Comunicaciones II. Modulo II Redes multiservicios conmutadas. Tema 4 Redes móviles, redes 3G y B3G.

[10] Open EPC –A Short OverviewProf. Dr. Thomas Magedanz, TU Berlin/Fraunhofer FOKUS Marius Corici, Fraunhofer FOKUS Dragos Vingarzan, Fraunhofer FOKUS.

[11] Mobile Services Network Technology Evolution and the role of IMS. George Korinthios, PhD Core Network New Technologies Manager COSMOTE S.A.

[12] 3GPP Mobile Broadband Innovation Path to 4G: Release 9, Release 10 and Beyond: HSPA+, SAE/LTE and LTE-Advanced. 3G Americas.

[13] 3GPP Radio Access Networks LTE-Advanced Status Takehiro Nakamura
3GPP TSG-RAN Chairman. September 2011.

[14] ITU global standard for international mobile telecommunications ´IMT-Advanced . Key features of ´IMT-Advanced.
http://www.itu.int/ITU-R/index.asp?category=information&rlink=imtadvanced&lang=en

[15] Question ITU-R 229-1/8 18-07-00xx-00-0000_IMT_Advanced_d3

[16] ITU Academy Portal Distance Learning on New Generation Network Management Approach. Semana_02_NGN_GET.

[17] Las Telecomunicaciones y la Movilidad en la Sociedad de la Información. Telefónica I+D. a iniciativa de AHCIET. Febrero 2005.

[18] The 3G IP Multimedia Subsystem (IMS) Merging the Internet and the Cellular Worlds Second Edition. Gonzalo Camarillo, Miguel A. García-Martín.

[19] RFC 3261. Session Initiation Protocol. IETF. Junio 2002.

[20] RFC 3264 Session Description Protocol IETF. Junio 2002.

[21] The IMS. IP Multimedia concepts and services. Second & third Edition. Miikka Poikselkä , Georg Mayer. Wiley & Sons. 2009.

[22] 3GPP TS 33.210 V11.3.0 3G security; Network Domain Security (NDS); IP network layer security(Release 11).

[23] 3GPP TS 33.102 3G security; Security architecture. Release 11.

[24] 3GPP TS 33.203 V11.0.0 3G security; Access security for IP-based services (Release 11).

[25] IP Multimedia Subsystem Handbook (IMS) Edited by Syed A. Ahson Mohammad Ilyas CRC Press.Taylor & Francis Group.

[26] 3GPP TS 23.228 V11.2.0 IP Multimedia Subsystem (IMS); Stage 2 (Release 11)

[27] 3GPP TS 23.218 V11.1.0 IP Multimedia (IM) session handling;IM call model; Stage 2 (Release 11).

[28] 3GPP TS 29.163 V11.0.0 Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks. (Release 11).

[29] 3GPP TS 29.162 V10.3.0 Interworking between the IM CN subsystem and IP networks (Release 10)

[30] 3GPP TS 23.203 V11.2.0 Policy and charging control architecture (Release 11).

[31] 3GPP TS 23.002 V9.1.0 Network architecture (Release 9)

[32] 3GPP TS 23.167 V11.4.0 IP Multimedia Subsystem (IMS) emergency sessions (Release 11)

[33] 3GPP TS 32.240 V11.2.0 Charging management;Charging architecture and principles (Release 11)

[34] 3GPP TS 32.260 V11.2.1 Charging management;IP Multimedia Subsystem (IMS) charging

(Release 11)

[35] 3GPP TS 32.296 V11.2.0 Online Charging System (OCS): Applications and interfaces (Release 11)

[36] 3GPP TS 24.228 V5.15.0 Signalling flows for the IP multimedia call control based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); (Release 5).

[37] 3GPP TS 24.229 V10.4.0 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); (Release 10).

[38] RFC 3261 SIP: Session Initiation Protocol

[39] RFC2617 HTTP Authentication: Basic and Digest Access Authentication.

[40] Proyecto piloto de colaboración para la adaptación de las redes móviles actuales a las especificaciones de IMS. Ericson AB –Orange Junio 2012.

[41] How NGNs Enable Advanced Telco Services: The Path to the Managed Cloud
Author: Steven Hawley Pyramid Research June 2012

[42] Q.1912.5B: Interworking between session initiation protocol (SIP) and bearer independent call control protocol (BICC) or ISDN user part (ISUP): Protocol implementation conformance statement (PICS).

[43] Orange Spain IMS solution - Ericsson Solution Description. Junio 2012